Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

МОНИТОРИНГ И АДМИНИСТРИРОВАНИЕ СЕТИ УНИВЕРСИТЕТА СРЕДСТВАМИ SYSTEM CENTER CONFIGURATION MANAGER

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 557

Екатеринбург 2019

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующий кафедрой ИС
_____ И. А. Суслова
«____» _____ 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

МОНИТОРИНГ И АДМИНИСТРИРОВАНИЕ СЕТИ УНИВЕРСИТЕТА СРЕДСТВАМИ SYSTEM CENTER CONFIGURATION MANAGER

Исполнитель:
обучающийся группы № ЗИБ–501 И. С. Зорин
Руководитель:
старший преподаватель С. В. Ченушкина
Нормоконтролер: С. Ю. Ярина

Екатеринбург 2019

АННОТАЦИЯ

Выпускная квалификационная работа состоит из руководства по управлению ИТ-инфраструктурой университета и пояснительной записки на 61 странице, содержащей 32 рисунков, 36 источников литературы.

Ключевые слова: ИТ-ИНФРАСТРУКТУРА, MS SCCM, МОНИТОРИНГ, АДМИНИСТРИРОВАНИЕ СЕТИ

Зорин И. С. Мониторинг и администрирование сети университета средствами System Center Configuration Manager: выпускная квалификационная работа / И. С. Зорин; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2019. — 61 с.

Цель работы: провести мониторинг и настройку серверов и рабочих станций компьютерной сети университета средствами System Center Configuration Manager и подготовить обучающее руководство по его использованию.

В рамках выполнения выпускной квалификационной работы были проанализированы источники и представленные на рынке программные решения по мониторингу и администрированию сети предприятия; выбран и настроен программный комплекс System Center Configuration Manager; проведен мониторинг компьютерной сети с составлением соответствующих отчетов; настроена возможность удаленного администрирования серверов и рабочих станций; подготовлены обучающие инструкции по работе с комплексом с использованием виртуального образа и в реальной инфраструктуре РГППУ; реализовать интерфейс руководства в выбранных средствах реализации.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Оснащенность корпоративной информационно-технологической инфраструктуры в соответствии с последними инновационными разработками в области информационных технологий — устойчивая тенденция последнего десятилетия.

В постоянной гонке за уникальными преимуществами в условиях жесткой конкуренции и роста потребностей общества в новых услугах, предприятия вынуждены прибегать к модернизации, проводя ее ускоренными темпами, внедряя новейшие системы управления бизнес-процессами, приобретая различное телекоммуникационное оборудование, оборудование систем связи и передачи данных, совершенствуя корпоративные сети и развивая технологические процессы. Интенсивный подход стал определяющим в отношении стратегии развития бизнеса: увеличение производительности, сокращение сроков окупаемости новых проектов, ускорение процесса обработки информации и реакции на события и т. д.

Данные опросов, проведенных независимо компанией HP и изданием Information Week Global CIO, сходятся на цифре в 70 % от всего объема средств годового бюджета, выделенного на развитие ИТ-инфраструктуры, которые уходят на обслуживание и поддержку существующих на предприятии сетей и телекоммуникационного оборудования [2]. При этом компания Lan Technologies Inc. обращает внимание на 70% случаев простоя технологических процессов в год, которые происходят по причине сбоев в работе на физическом уровне сети.

И все же несмотря на то, что существует множество решений, позволяющих проводить мониторинг сети и сетевого оборудования, оценить эффективность ее работы достаточно сложно. Даже поиск причин аварии вызывает трудности у специально неподготовленного персонала, поскольку приходится просматривать и анализировать гигантские журналы событий, со-

держащие устрашающее количество сообщений системы, на что зачастую тратится около 40% рабочего времени.

Федеральное государственное автономное образовательное учреждение высшего образования (ФГАОУ ВО) «Российский государственный профессионально-педагогический университет» (РГППУ) — это высшее учебное заведение Екатеринбурга, в состав которого входят институты, колледж, филиал и представительства в различных городах Российской Федерации (РФ).

На данный момент ФГАОУ ВО «РГППУ» насчитывает порядка 600 рабочих станций и 20 серверов. Управление данной инфраструктурой возложено на отдел развития информационных сетей и технического сопровождения (РИС и ТС), основная цель которого — обеспечение качественного и бесперебойного режима информационно-коммуникационной системы и сетевого оборудования.

Обслуживание вручную ограниченным количеством сотрудников отдела нецелесообразно, в связи с чем возникла необходимость в развертывании специального программного решения и обучения специалистов отдела по его использованию в процессе выполнения производственных задач.

Предоставление технологических решений — экономичных и соответствующих потребностям бизнеса — важнейшая задача ИТ-отделов во всем мире. Поскольку организации растут и приспосабливаются к изменению рыночной ситуации, ИТ- среда должна быть гибкой и обеспечивать техническую поддержку бизнесу. Бизнес-пользователи хотят, чтобы сотрудники ИТ-отделов оперативно реагировали на постоянно меняющиеся потребности и вели «непрерывное обслуживание [1].

Продукт System Center представляет собой комплексное решение для управления современной ИТ-инфраструктурой предприятия. Решение System Center Configuration Manager (SCCM) позволяет осуществлять развертывание и настройку программного обеспечения (ПО), а также организацию и контроль взаимодействия пользователей с мобильными, физическими и виртуальными средами с различных устройств. Оно обладает всеми преимуще-

ствами предыдущих версий, а также включает новые и расширенные возможности оценки клиентов, развертывания операционных систем (ОС), учета ресурсов, управления обновлениями и применения настроек. Использование данного программного средства позволит повысить проанализировать текущее состояние рабочих станций и получить возможность их удаленного управления.

Объект исследования: возможность мониторинга и удаленного администрирования серверов и рабочих станций компьютерной сети университета.

Предмет исследования: мониторинг и администрирование компьютерной сети университета с использованием специализированного программного обеспечения и сопроводительной обучающей документацией.

Цель работы: провести мониторинг и настройку серверов и рабочих станций компьютерной сети университета средствами System Center Configuration Manager и подготовить обучающее руководство по его использованию.

Для достижения поставленной цели в работе определены следующие задачи:

1. Проанализировать источники и представленные на рынке программные решения по мониторингу и администрированию сети предприятия.
2. Настроить программный комплекс и провести мониторинг компьютерной сети с составлением соответствующих отчетов.
3. Настроить возможность удаленного администрирования серверов и рабочих станций с использованием программного комплекса с пробной установкой программного обеспечения.
4. Подготовить обучающие инструкции по работе с комплексом с использованием виртуального образа и в реальной инфраструктуре РГППУ;
5. Реализовать интерфейс руководства в выбранных средствах реализации.

1 ОБЗОР ТЕХНОЛОГИЙ МОНИТОРИНГА И АДМИНИСТРИРОВАНИЯ СЕТИ

1.1 Необходимость применения систем мониторинга и администрирования сети

Мониторинг серверов, выполняемых на них приложений и сетевых устройств, поможет заблаговременно узнать о потенциальных неисправностях и предотвратить их последствия. Отслеживая функционирование сети и сохраняя предысторию ее работы, администратор к тому же может предоставить точную информацию пользователям, у которых иногда складывается неверное представление о частоте появления различных неисправностей. Не менее важно, что сетевой мониторинг позволяет получать точные сведения о событиях в сети, а также времени и источниках обращений в сеть. Итак, существует два типа мониторинга. Первый из них мы будем называть оперативным мониторингом (operations monitoring), а второй — мониторингом безопасности (security monitoring) [11].

Крупные предприятия иногда делят эти два типа мониторинга на два отдельных процесса, выполняемые сотрудниками производственных подразделений и ИТ-безопасности, но малые и средние компании по ряду причин чаще организуют общий процесс мониторинга. Независимо от размера бюджета и числа сотрудников, сети малых и средних компаний обычно не нуждаются в таком же уровне текущего оперативного мониторинга, как в крупных корпорациях. Сети малых предприятий загружены не столь интенсивно, как корпоративные, и обслуживать их не так сложно [4]. Кроме того, технические проекты малых компаний проще, и они не нуждаются в детальном анализе тенденций и отчетах, необходимых в учреждениях с более медленными процедурами принятия решений.

Сначала рассмотрим те различные устройства и системы малого предприятия, которые необходимо контролировать как в целях безопасности, так и по производственным причинам, и определим типичные источники отслеживаемых данных, в том числе журналы событий Windows, Syslog и SNMP. Далее покажем, как построить элементарное решение для мониторинга сети с помощью бесплатных и недорогих инструментов [19].

1.2 Объекты мониторинга

В целях безопасности полезно контролировать все сетевые устройства (например, брандмауэры, шлюзы, VPN-устройства, беспроводные узлы доступа — AP) на границе сети — периметре безопасности, а также любые серверы, на которых размещаются информация и процессы, требующие конфиденциальности или целостности [20].

Для производственных целей следует контролировать все устройства и серверы, отказоустойчивость которых важна для нормальной работы предприятия (рисунок 1).

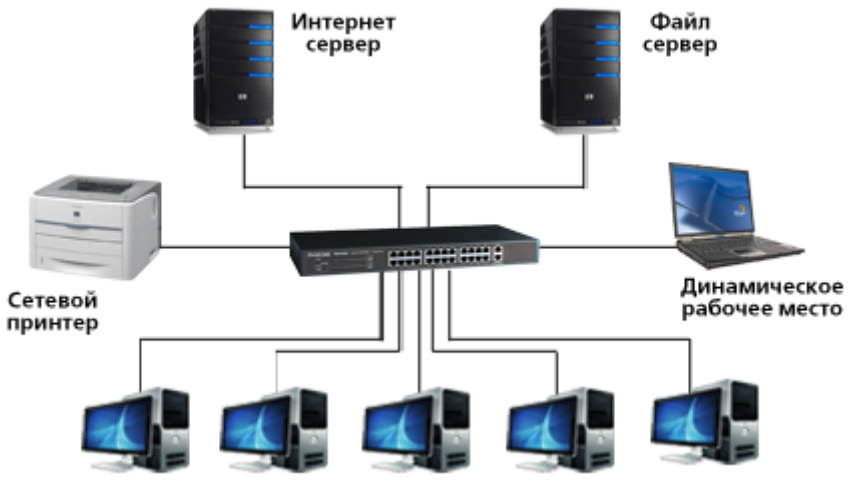


Рисунок 1 — Пример карты сети

Для Windows необходим мониторинг не только операционной системы, но и важных приложений, таких как Microsoft Exchange Server, Microsoft ISA Server, Microsoft IIS и Microsoft SQL Server [21].

Полезно контролировать высокоуровневые приложения (например, Microsoft SharePoint Portal Server), если таким образом удается обнаружить важные события, относящиеся к сфере безопасности или производства, которые могут остаться незамеченными средствами нижележащих баз данных, на которых они работают.

1.3 Методы мониторинга и администрирования

Методы мониторинга, основанные на маршрутизаторе — жёстко заданы (вшиты) в маршрутизаторах и, следовательно, имеют низкую гибкость. Краткое описание наиболее часто используемых методов такого мониторинга приведены ниже. Каждый метод развивался много лет, прежде чем стать стандартизованным способом мониторинга [12].

Протокол простого сетевого мониторинга (SNMP), RFC 1157

SNMP — протокол прикладного уровня, который является частью протокола TCP/IP. Он позволяет администраторам руководить производительностью сети, находить и устранять сетевые проблемы, планировать рост сети [10]. Он собирает статистику по трафику до конечного хоста через пассивные датчики, которые реализуются вместе с маршрутизатором. В то время, как существуют две версии (SNMPv1 и SNMPv2), данный раздел описывает только SNMPv1. SNMPv2 построен на SNMPv1 и предлагает ряд усовершенствований, таких как добавление операций с протоколами. Стандартизируется ещё один вариант версии SNMP. Версия 3 (SNMPv3) находится на стадии рассмотрения.

Для протокола SNMP присущи три ключевых компонента: управляемые устройства (Managed Devices), агенты (Agents) и системы управления сетью (Network Management Systems – NMSs). Они показаны на рисунке 2.

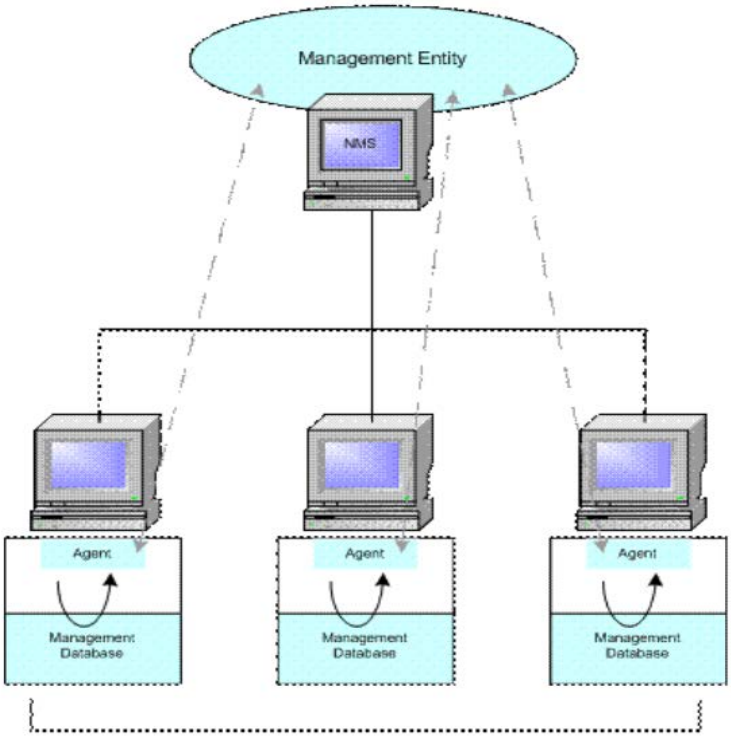


Рисунок 2 — Компоненты протокола простого сетевого мониторинга

Удалённый мониторинг (RMON), RFS 1757

RMON включает в себя различные сетевые мониторы и консольные системы для изменения данных, полученных в ходе мониторинга сети [20]. Это расширение для SNMP информационной базы данных по управлению (MIB). В отличии от SNMP, который должен посылать запросы о предоставлении информации, RMON может настраивать сигналы, которые будут «мониторить» сеть, основанную на определённом критерии. RMON предоставляет администраторам возможности управлять локальными сетями также хорошо, как удалёнными от одной определённой локации/точки. Его мониторы для сетевого уровня приведены ниже. RMON имеет две версии RMON и RMON2. Однако в данной статье говорится только о RMON. RMON2 позволяет проводить мониторинг на всех сетевых уровнях. Он фокусируется на IP-трафике и трафике прикладного уровня.

Хотя существует три ключевых компонента мониторинговой среды RMON, здесь приводятся только два из них. Они показаны на рисунке 3.

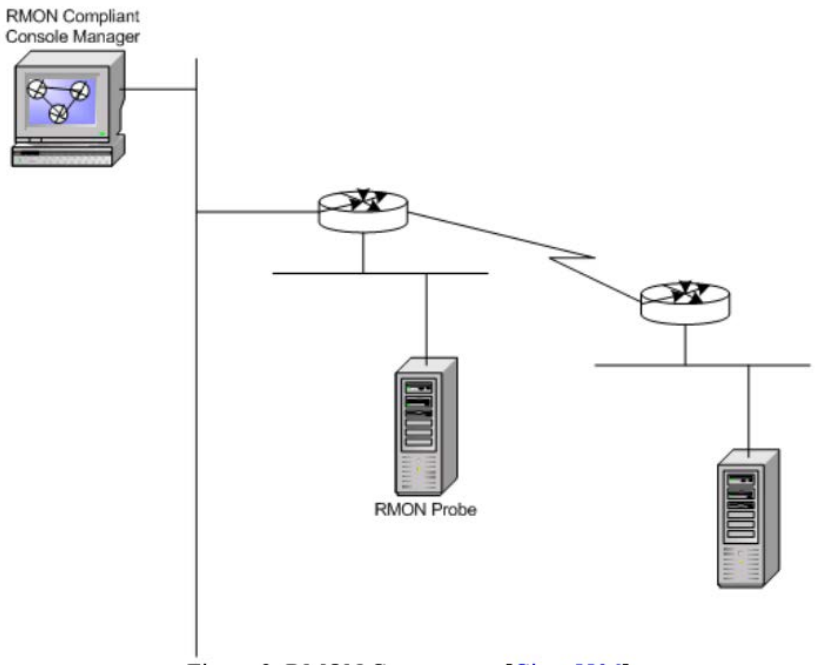


Рисунок 3 — Компоненты удаленного мониторинга

Два компонента RMON это датчик, также известный как агент или монитор, и клиент, также известный как управляющая станция (станция управления). В отличии от SNMP датчик или агент RMON собирает и хранит сетевую информацию. Датчик — это встроенное в сетевое устройство (например, маршрутизатор или переключатель) программное обеспечение. Датчик может запускаться также и на персональном компьютере. Датчик должен помещаться для каждого различного сегмента локальной или глобальной сети, так как они способны видеть трафик, который проходит только через их каналы, но они не знают о трафике за их приделами. Клиент — это обычно управляющая станция, которая связана с датчиком, использующим SNMP для получения и коррекции RMON-данных [13].

RMON использует 9 различных групп мониторинга для получения информации о сети:

1. Statistics — статистика, измеренная датчиком для каждого интерфейса мониторинга для данного устройства.

2. History — учёт периодических статистических выборок из сети и хранение их для поиска.

3. Alarm — периодически берёт статистические образцы и сравнивает их с набором пороговых значений для генерации события.

4. Host — содержит статистические данные, связанные с каждым хостом, обнаруженным в сети.

5. HostTopN — готовит таблицы, которые описывают вершину хостов (главный хост).

6. Filters — включает фильтрацию пакетов, основываясь на фильтровом уравнении для захвата событий.

7. Packet capture — захват пакетов после их прохождения через канал.

8. Events — контроль генерации и регистрация событий от устройства.

9. Token ring — поддержка кольцевых лексем.

Как установлено выше, RMON, строится на протоколе SNMP. Хотя мониторинг трафика может быть выполнен при помощи этого метода, аналитические данные об информации, полученные SNMP и RMON имеют низкую производительность. Утилита Netflow, которая обсуждается в следующем разделе, работает успешно со многими пакетами аналитического программного обеспечения, чтобы сделать работу администратора намного проще.

Netflow, RFS 3954

Netflow — это расширение, которое было представлено в маршрутизаторах Cisco, которые предоставляют возможность собирать IP сетевой трафик, если это задано в интерфейсе [24].

Анализируя данные, которые предоставляются Netflow, сетевой администратор может определить такие вещи как: источник и приёмник трафика, класс сервиса, причины переполненности. Netflow включает в себя 3 компонента: FlowCaching (кеширующий поток), FlowCollector (собиратель информации о потоках) и Data Analyzer (анализатор данных). Рисунок 4 показывает инфраструктуру Netflow. Каждый компонент, показанный на рисунке 4, объясняется ниже.

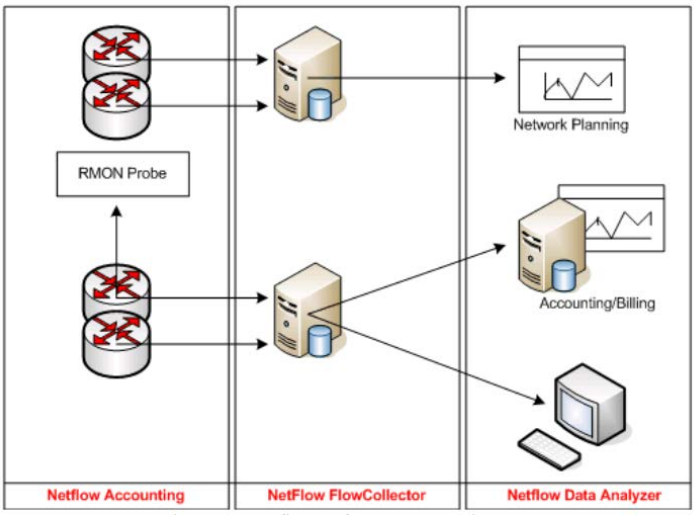


Рисунок 4 — Инфраструктура NetFlow

FlowCaching анализирует и собирает данные о IP потоках, которые входят в интерфейс, и преобразует данные для экспорта.

WMI (Windows Management Instrumentation или Инструментарий управления Windows) – это технология для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows (рисунок 5).

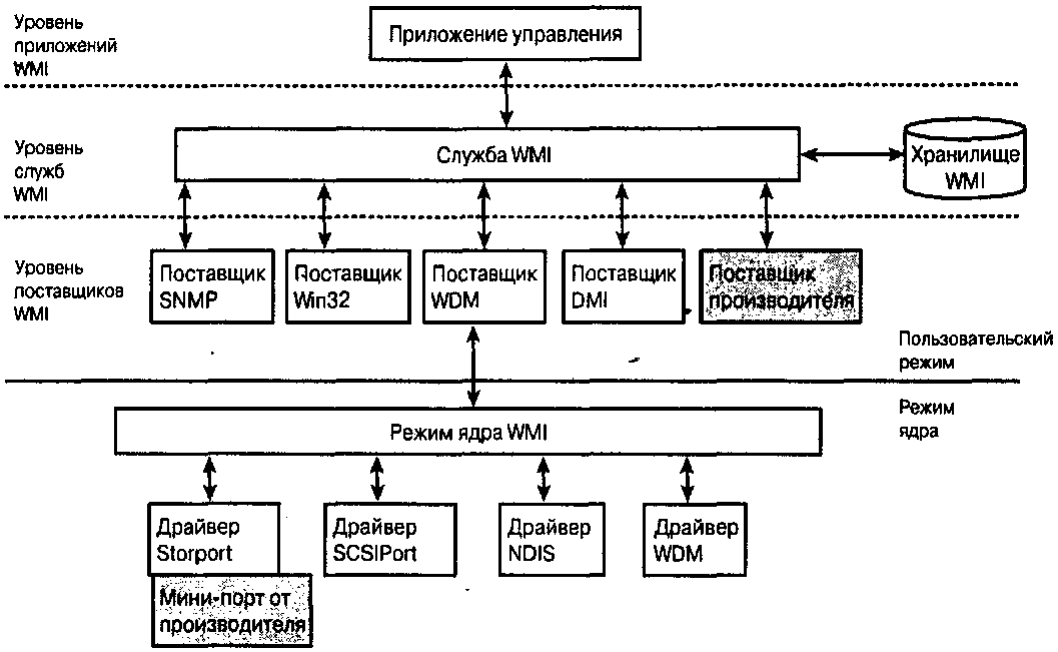


Рисунок 5 — Архитектура инструментария управления Windows

Технология WMI — это расширенная и адаптированная под Windows реализация стандарта WBEM, принятого многими компаниями, в основе которого лежит идея создания универсального интерфейса мониторинга и

управления различными системами и компонентами распределенной информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML. WMI является мощным инструментом для администрирования операционных систем семейства Windows при помощи скриптов. С помощью WMI можно управлять устройствами, учетными записями, сервисами, процессами, сетевыми интерфейсами и другими программами, которые расширяют базовую структуру WMI своими классами. Помимо скриптов WMI может применяться и в полноценных программах, то есть программисты могут внедрять запросы к WMI в исполняемый код, завязывая свою программу с работой WMI, благодаря чему программа становится проще и легче, но зависимой от правильности работы Windows Management Instrumentation.

1.4 Обзор программ мониторинга и администрирования сети

Novell ZENworks Configuration Management — комплексное управление IT-системами для уменьшения общей стоимости владения. Интуитивно понятный web-интерфейс в сочетании с функциями безопасного дистанционного управления и делегированного администрирования позволяет персоналу службы технической поддержки быстро помогать пользователям (рисунок 6).

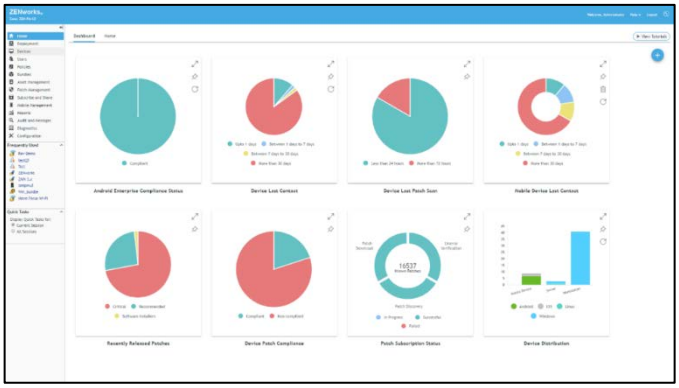


Рисунок 6 — Окно программы Novell ZENworks Configuration Management

Основные функции:

- централизованная установка и обновление ПО и ОС;
- инвентаризация программного и аппаратного обеспечения;
- удаленное управление рабочими станциями и серверами.

Управление осуществляется на основании системных политик, единых в масштабе всей сети. Управление станциями осуществляется из общей консоли.

SolarWinds Network Performance Monitor — система мониторинга сетей и активного сетевого оборудования (рисунок 7).

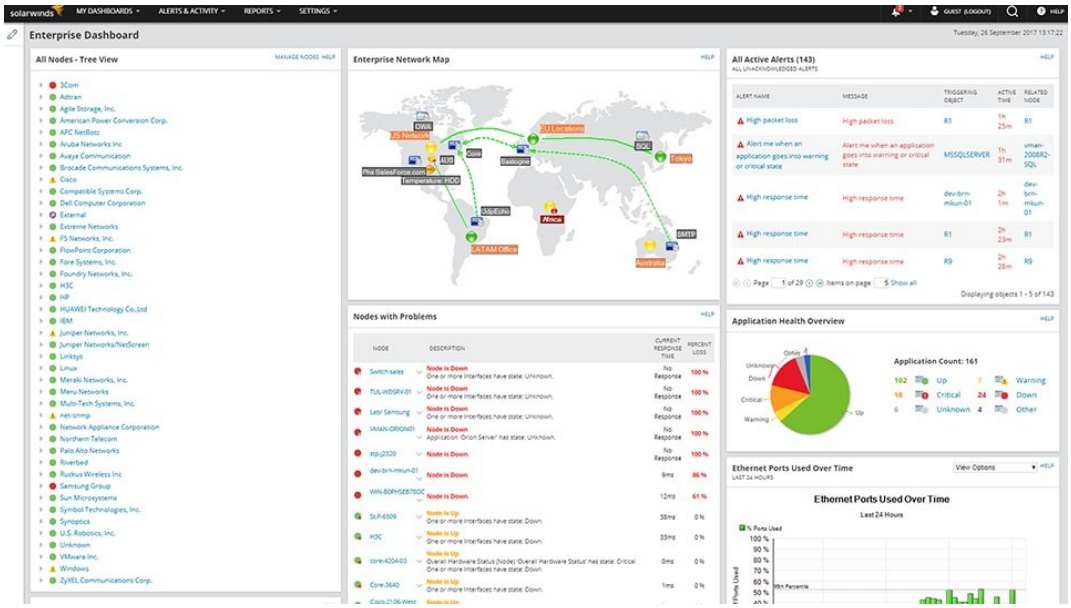


Рисунок 7 — Окно программы SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor позволяет отслеживать сетевую производительность в режиме реального времени. А также осуществляет выявление, диагностику и решение проблем быстродействия до возникновения простоев в работе. Благодаря наличию динамических карт топологии сети и автоматическому обнаружению ее компонентов администратор может легко масштабировать сеть, приводя в соответствие важные процессы по мере ее роста.

Основные функции:

1. Автоматическое обнаружение сети. Программа позволяет легко планировать процессы автоматического сканирования сети, обнаруживать

новые сетевые устройства и осуществлять мониторинг критически важного оборудования;

2. Поддержка устройств от различных вендоров. Network Performance Monitor поддерживает гетерогенные сети и устройства от ведущих производителей оборудования;

3. Мониторинг производительности и доступности сети. Программа позволяет отслеживать доступность и индикаторы производительности интерфейса и сетевых устройств, такие как нагрузка на полосу пропускания, центральный процессор и память, задержки, ответы, потеря пакетов — по каждому оборудованию с поддержкой SNMP и WMI;

4. Интеллектуальные уведомления. Продукт поддерживает оповещения о событиях, условиях и состояниях сетевых устройств. При необходимости администратор может заблокировать уведомления на основе зависимостей и топологии и получать оповещения только по важным сетевым проблемам;

5. Быстрое развертывание. Network Performance Monitor загружается и устанавливается менее чем за час в три простых шага.

Программно-аппаратное решение Dell KACE K1000 Management Appliance – комплексное устройство управления сетевыми системами IT инфраструктуры предприятия. Данное устройство рассчитано на предприятия, где число конечных узлов от 100 до 20 тысяч единиц (рисунок 8).

Рисунок 8 — Внешний вид программно-аппаратного комплекса Dell KACE K1000 Management Appliance и программного обеспечения

С помощью устройства можно управлять серверами, настольными компьютерами и ноутбуками на основе простого пользовательского интерфейса. При этом осуществляется централизованное управление единой консолью для сетей, построенных на оборудовании от разных производителей, разнообразной архитектуры, различных поколений и версий.

Основные функции:

- обнаружение и инвентаризация всего оборудования и программного обеспечения во всей сети;
- управление патчами для автоматического анализа уязвимых мест и установки обновлений;
- управление ресурсами для осуществления комплексного отслеживания ресурсов и отчетов о соответствии нормативными требованиями;
- групповые оповещения для уведомлений пользователей о важных событиях, например, таких как перебой в работе службы электронной почты;
- распространение программного обеспечения включает возможности удаленного распределения и установки приложений и цифровых ресурсов;
- удаленное управление позволяет централизованно заниматься устранением неисправностей без необходимости выезда на место.

CiscoWorks LMS — это семейство программных продуктов для упрощения настройки, мониторинга и диагностики сетей, построенных на базе продукции Cisco. LMS является интегрированной системой, которая предоставляет данные о сетевых устройствах для других информационных систем, автоматизирует рутинные задачи по управлению сетью, обеспечивает сбор и предоставление данных о загрузке устройств и предоставляет функции для локализации сетевых проблем и их диагностики. Все компоненты системы используют общий модуль хранения информации об устройствах, что значи-

тельно упрощает настройку решения и его интеграцию с существующими информационными системами компании (рисунок 9).

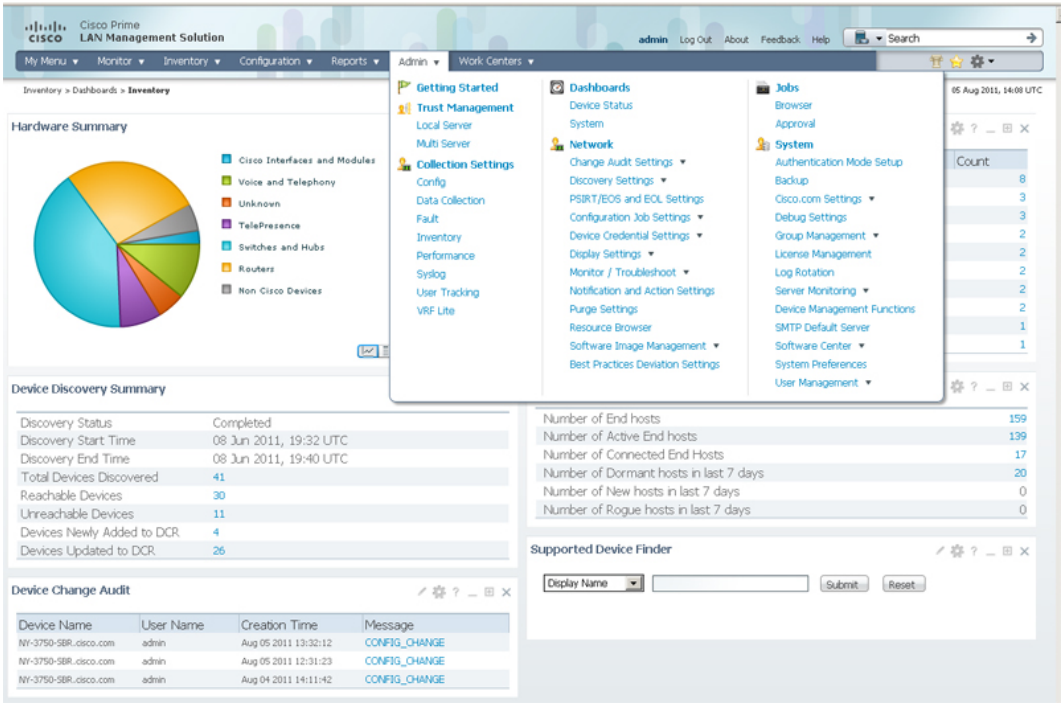


Рисунок 9 — Окно программы CiscoWorks

Решение CiscoWoks LMS состоит из нескольких приложений. Пользователь может установить все приложения или только некоторые из них в соответствии со своими задачами. Все приложения поставляются в одном пакете и функционируют в соответствии с единой лицензией (за исключением приложения Healthand Utilization Monitor, для использования которого требуется приобретение отдельной лицензии)

Naumen Network Manager — комплексное решение для мониторинга ИТ-инфраструктуры и управления сетями любого масштаба. Naumen Network Manager сканирует сеть, отслеживая состояние физических и виртуальных серверов, рабочих станций, маршрутизаторов, коммутаторов, других устройств, сервисов и приложений. Платформа объединяет несколько сотен компонентов для сетевого управления, позволяющих работать с тревогами, применять оповещения и обработчики событий, создавать отчеты и диаграммы, строить карты сети, выполнять задачи по составленному расписанию и многое другое (рисунок 10).

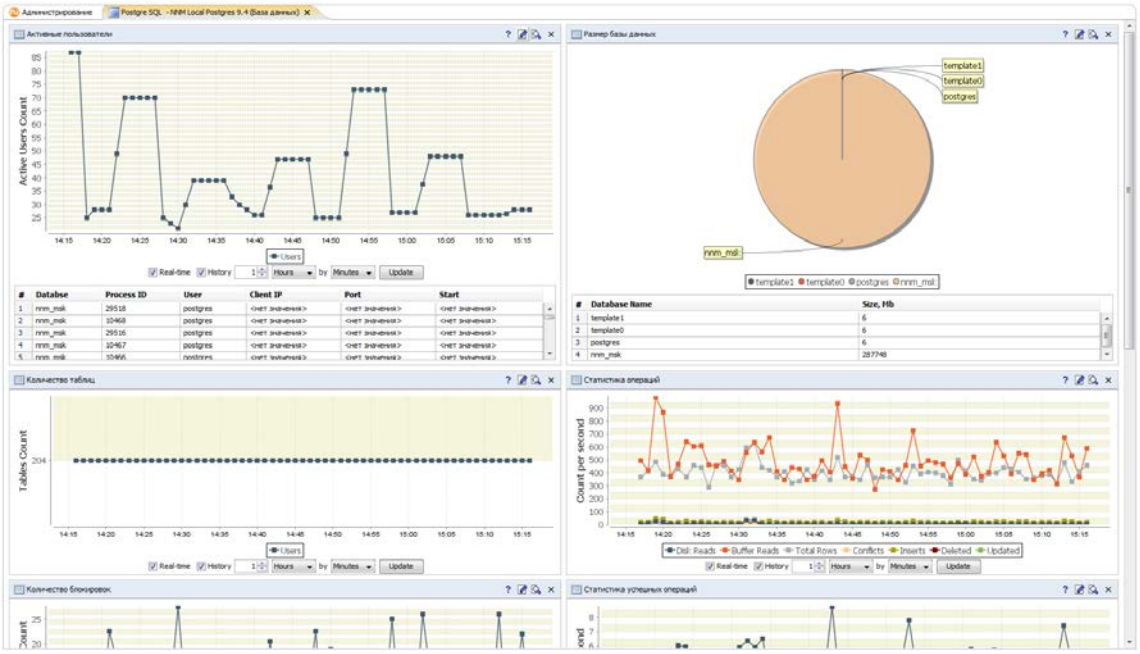


Рисунок 10 — Окно программы Naumen Network Manager

Основные возможности:

- мониторинг сетей;
- мониторинг серверов;
- мониторинг приложений и сервисов;
- мониторинг маршрутизаторов;
- мониторинг виртуальной инфраструктуры;
- мониторинг VOIP и проверка IP SLA;
- мониторинг баз данных;
- мониторинг и управление по SNMP;
- управление IT-активами.

Ivanti Endpoint Manager (ранее LANDesk Management Suite) — комплексная система инвентаризации/управления парком ПК и серверов. Решение позволяет ИТ-администраторам получить комплексную инвентарную информацию о компьютерном парке компании, автоматизировать задачи по распространению программного обеспечения и операционных систем, быстро устранять проблемы пользователей при помощи технологий удаленного подключения, отслеживать программные и аппаратные активы (рисунок 11).

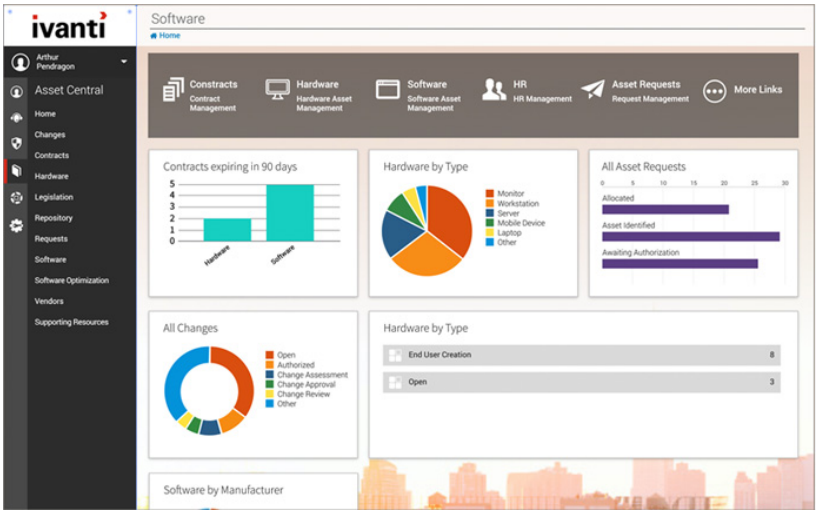


Рисунок 11 — Окно программы Ivanti Endpoint Manager

Основные функции:

- активное, пассивное и безагентное обнаружение и инвентаризация;
- конфигурация и управление политиками;
- удаленное управление;
- автоматизированная установка ОС и ПО;
- система оповещений о событиях;
- создание отчетов;
- портал самообслуживания;
- сканирование и исправление угроз безопасности (при наличии модуля Endpoint Security for Endpoint Manager);
- оптимизация используемого ПО, удаление неиспользуемых продуктов, оптимизация затрат на закупку лицензий (при наличии модуля Asset Intelligence).

System Center Configurations Manager (SCCM) позволяет осуществлять развертывание и настройку ПО, организацию и контроль взаимодействия пользователей с мобильными, физическими и виртуальными средами с различных устройств. Оно обладает всеми преимуществами предыдущих версий, а также включает новые и расширенные возможности оценки клиентов, развертывания операционных систем, учета ресурсов, управления обновлениями и применения настроек.

SCCM помогает обеспечить продуктивную работу пользователей, предоставляя оптимальные возможности для работы в любом месте и на любом устройстве [5].

Благодаря консолидации всех возможностей управления клиентами и функций безопасности в единой инфраструктуре, обеспечиваемой Configuration Manager, организация сможет оптимизировать свою деятельность по управлению ИТ (рисунок 12).

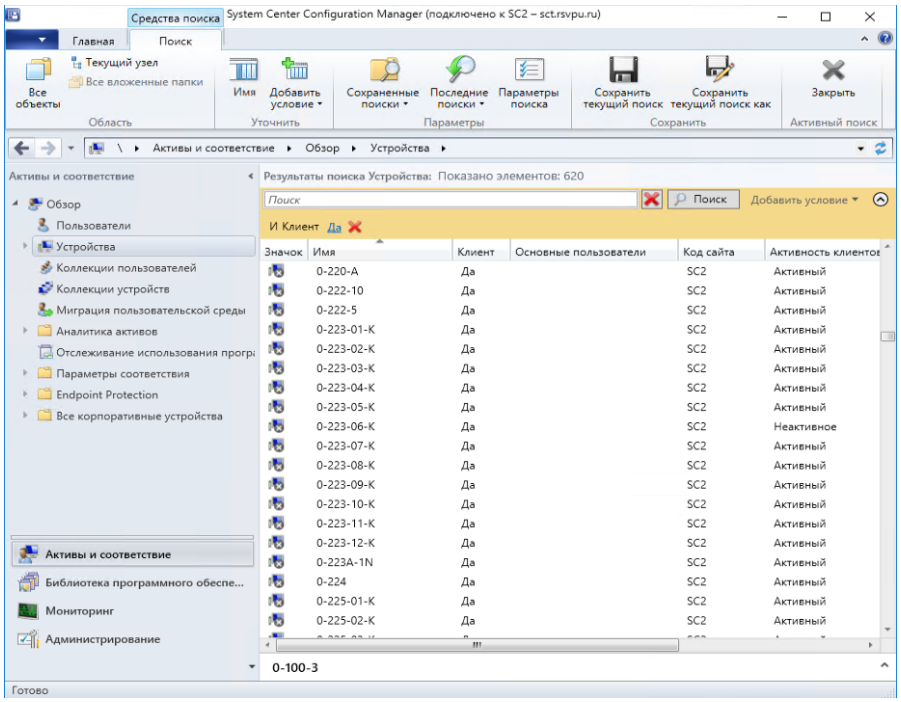


Рисунок 12 — Окно программы System Center Configurations Manager

Zabbix

Zabbix — бесплатная системы мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования. Для хранения данных используется MySQL, PostgreSQL, SQLite или Oracle (рисунок 13) [14]. Веб-интерфейс написан на PHP. ZABBIX поддерживает несколько видов мониторинга:

- Simple checks — может проверять доступность и реакцию стандартных сервисов, таких как SMTP или HTTP без установки какого-либо программного обеспечения на наблюдаемом хосте;

- ZABBIX agent — может быть установлен на UNIX-подобных или Windows хостах для получения данных о нагрузке процессора, использования сети, дисковом пространстве и т.д.;
- External check — выполнение внешних программ. ZABBIX также поддерживает мониторинг через SNMP.

Возможности:

- распределенный мониторинг вплоть до 1000 узлов, конфигурация младших узлов полностью контролируется старшими узлами, находящихся на более высоком уровне иерархии;
- сценарии на основе мониторинга;
- автоматическое обнаружение;
- централизованный мониторинг лог-файлов;
- поддержка SNMP ловушек;
- поддержка IPMI;
- поддержка мониторинга JMX приложений из коробки;
- поддержка выполнения запросов в различные базы данных без необходимости использования скриптовой обвязки;
- расширение за счет выполнения внешних скриптов;
- возможность создавать карты сетей.

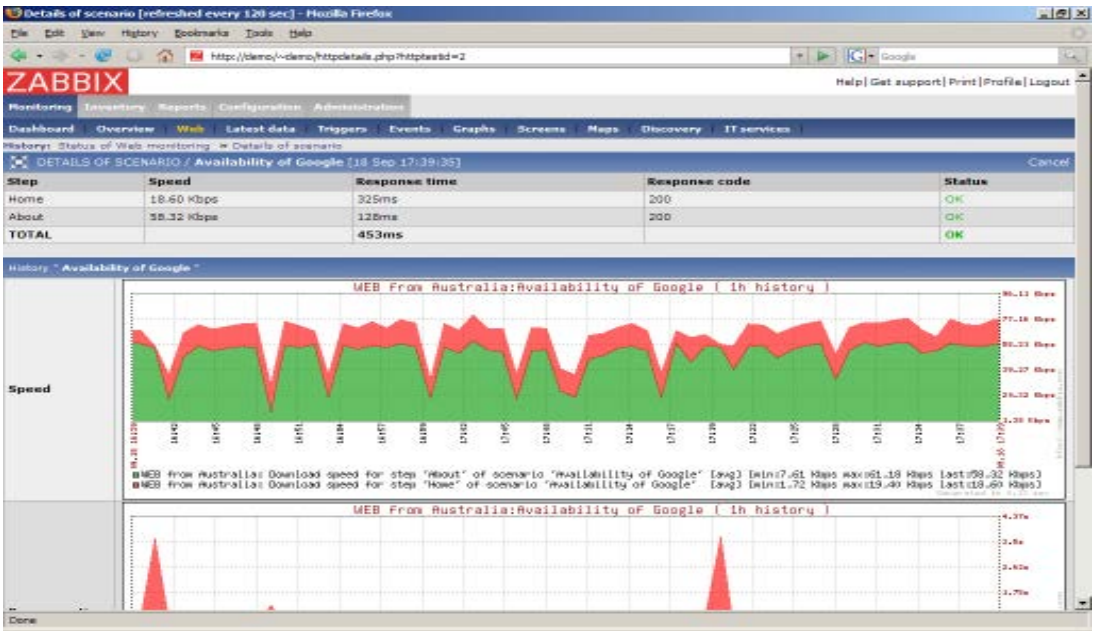


Рисунок 13 — Окно программы Zabbix

Friendly Pinger

Friendly Pinger — это бесплатное приложение для администрирования, мониторинга и инвентаризации компьютерных сетей (рисунок 14) [31].

Возможности Friendly Pinger:

- визуализация компьютерной сети в красивой анимационной форме;
- отображение, какие компьютеры включены, а какие нет;
- пингование всех устройств за раз;
- оповещение в случае остановки/запуска серверов;
- инвентаризация программного и аппаратного обеспечения всех компьютеров в сети;
- слежение, кто «лазает» по Вашему компьютеру и какие файлы качает;
- назначение внешних команд (например, telnet, tracert, net.exe) устройствам;
- поиск HTTP, FTP, e-mail и других сетевых служб;
- отображение состояния сети на рабочем столе или Web странице;
- графический TraceRoute;
- открытие компьютеров в проводнике, в Total Commander'e или в FAR'e;
- функция «Создать дистрибутив» позволяет создать облегченную версию с Вашими картами и настройками [31].

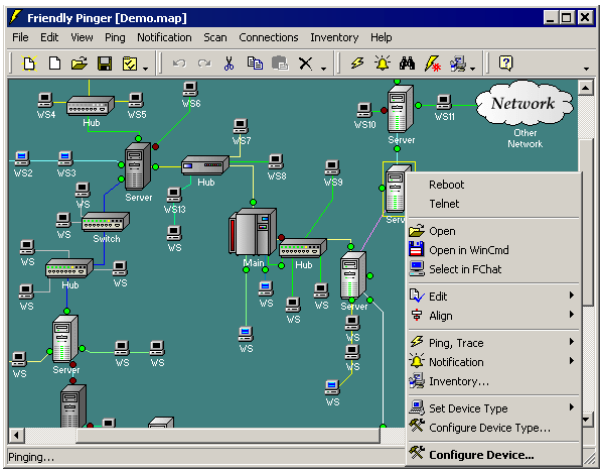


Рисунок 14 — Окно программы Friendly Pinger

Friendy Pinger — бесплатное средство мониторинга и инвентаризации небольших локальных сетей с поддержкой русского языка.

Кроме стандартных возможностей подобных программ, Friendly Pinger позволяет использовать встроенные команды, вызываемые из контекстного меню объекта на карте сети, и передать им некоторые внутренние переменные, что превращает программу в некий центр управления локальной вычислительной сетью (ЛВС), позволяющей легко и быстро выполнить, например, следующие действия:

- включить, выключить или перезагрузить удаленный компьютер;
- получить доступ к удаленному рабочему столу Windows или графической подсистеме Linux;
- получить доступ к удаленной командной строке Windows или Linux;
- выполнить подключения к различным удаленным сетевым службам;
- подключиться к серверу терминалов или серверу SSH;
- принудительно завершить любой процесс на отдельно взятом компьютере или на всех включенных компьютерах [15].

В целом, встроенные команды Friendly Pinger позволяют каждому системному администратору расширить возможности программы на свой вкус, и получить в свое распоряжение удобный инструмент управления локальной сетью [3].

1.5 Выводы по первой главе

Преимущества внедрения системы управления ИТ-инфраструктурой:

- повышение доступности и надежности критически важных IT-ресурсов;
- повышение эффективности работы сотрудников, за счет снижения временных затрат IT-персонала на рутинные операции;

- возможность оперативного анализа и контроля оборудования организации;
- сокращение времени ввода нового оборудования;
- снижение временных затрат на обновление, развертывание и настройку ПО.

Централизованный контроль устройств позволяет повысить безопасность сети, сократить время простоя систем и оборудования, удовлетворить требования, связанные с условиями лицензионных соглашений на ПО.

Программные продукты такие как: Friendly Pinger, 10-Strike LANState — представляют собой простые инструменты для мониторинга сети и инвентаризации аппаратного обеспечения. Но функционал данных инструментов весьма ограничен и не позволяет в полной мере управлять всей инфраструктурой организации.

Система Zabbix является универсальной системой мониторинга корпоративной сети. Однако в данном продукте отсутствует возможность удаленного подключения к рабочим станциям и серверам. Инвентаризационные данные аппаратного обеспечения, содержат лишь основную информацию о системе: загрузка процессора, использование дисков, использование памяти, информация о входящем/исходящем трафике, а также состояние основных служб Windows. Функция инвентаризации ПО — отсутствует.

Программный продукт CiscoWorks LMS предназначен в первую очередь для сетей, построенных на базе оборудования Cisco. Т. к. содержит множество инструментов, специально предназначенных для работы с данным оборудованием. В университете имеется ряд оборудования Cisco, но все же большая часть оборудования — других производителей.

Программные продукты, такие как Naumen Network Manager, Ivanti Endpoint Manager, SolarWinds Network Performance Monitor и Novell ZENworks Configuration Management, а также программно-аппаратный комплекс Dell KACE K1000 Management Appliance — являются мощными инструмен-

тами мониторинга ИТ-инфраструктуры предприятия, однако требуют весьма больших финансовых затрат на их приобретение.

Ключевым фактором выбора системы SCCM является доступность данного продукта для университета. Университет ежегодно приобретает лицензии на программные продукты Microsoft по подписке Microsoft Desktop Education ALNG LicSAPk OLVS. В данную подписку входят последние версии программных продуктов таких как: Windows, Windows Server, Office, SQL-server и т. д., в том числе пакет продуктов System Center. В связи с чем использование SCCM экономит средства университета на приобретение программного обеспечения для мониторинга и управления ИТ-инфраструктурой.

2 ОПИСАНИЕ ЭЛЕКТРОННОГО РУКОВОДСТВА

2.1 Описание основных задач по мониторингу и администрированию сети, выполняемых сотрудниками отдела

РГППУ обладает большим количеством компьютерных ресурсов, которые требую постоянного мониторинга и обслуживания. Качественно построенная система требует грамотного обслуживания сети квалифицированными специалистами и соблюдения норм и принципов работы, заложенных производителем программного обеспечения. Именно нарушение технологии решения тех или иных задач приводит к возникновению сбоев работы серверов и нарушению безопасности при доступе к данным.

Основными задачами по мониторингу и администрированию сети, выполняемые сотрудниками одела являются:

- мониторинг и анализ текущего состояния информационно-коммуникационной системы и сетевого оборудования;
- выявление и устранение неполадок в ходе эксплуатации компьютерного и сетевого оборудования;
- мониторинг состояния узлов локальной вычислительной сети университета, обработка и анализ полученных данных;
- выполнение работ по обновлению программного обеспечения;
- своевременное внесение необходимых изменений в настройки сетевого оборудования;
- обеспечение доступа к сети Интернет и сервисам электронной почты;
- выполнение работ по модернизации локальной вычислительной сети университета;
- учет и анализ случаев отказа в работе сетевого оборудования информационно-коммуникационной системы;

- выполнение мероприятий по обеспечению информационной безопасности и защите локальной вычислительной сети университета, компьютерного и сетевого оборудования путем администрирования прав доступа, применения антивирусного ПО и др.

Помимо этого, для выполнения задач по осуществлению работ по обеспечению структурных подразделений университета компьютерным оборудованием на отдел, возлагаются следующие функции:

- определение потребностей университета в обеспечении компьютерным оборудованием и программным обеспечением;
- выполнение работ по подготовке оборудования к эксплуатации (сборка, настройка, установка программного обеспечения и др.);
- организация работ по документационному учету компьютерного оборудования;
- информирование материально-ответственных лиц о необходимости модернизации, замены, списания компьютерного оборудования.

Мы разделяем задачу обслуживания компьютеров и серверов на две важных части: помощь пользователям в устранении возникающих проблем и проведение регламентных работ по обслуживанию сети.

Основные проблемы, которые возникают:

1. ПО устанавливается вручную сотрудниками отдела РИС и ТС на каждую рабочую станцию посредством запуска инсталляционного файла, расположенного на съемном носителе, либо на сетевом диске.
2. Нет возможности отслеживать использование ПО на рабочих станциях.
3. Обновления Microsoft устанавливаются на рабочих станциях и серверах из Центра обновления Windows, без контроля.
4. Антивирусное ПО, установленное на рабочих станциях — без централизованного управления и контроля.

5. Отсутствует сопоставление рабочих станций с учетными записями пользователей. Невозможно оперативно без использования скриптов определить на каких компьютерах работает пользователь.

6. Инвентаризация программного и аппаратного обеспечения производится посредством GLPI. В ходе эксплуатации данной системы было выявлено неудобство создания собственных отчетов. Т.к. для добавления дополнительных полей, требовалось изменение PHP кода;

7. Удаленный доступ к рабочей станции или серверу, осуществляется, путем запуска вручную оснастки MSTSC — «подключение к удаленному рабочему столу». Для подключения необходимо было знать сетевое имя, либо IP-адрес рабочей станции/сервера.

Возникла необходимость в процедуре контроля за состоянием серверов и оборудования, направленные на поддержание актуального состояния программных средств. В рамках проекта решались следующие задачи:

- автоматизация развертывания ПО на рабочих станциях университета;
- создание системы распространения обновлений ОС и ПО в рамках системы управления конфигурациями;
- сбор инвентаризационных данных о программном и аппаратном обеспечении с рабочих станций и серверов;
- контроль использования программного обеспечения;
- развертывание функционала антивирусной защиты конечных точек Endpoint Protection в рамках стандартного клиента SCCM;
- предоставление сотрудникам ИТ-службы функционала удаленного управления рабочими станциями;
- настройка шаблонов отчетности в рамках штатных возможностей SCCM, в частности, отчетов по аппаратному обеспечению и идентификации пользователей рабочих станций.

Необходимо разработать технологию обслуживания компьютеров и серверов, при проведении которой контролировались различных параметры функционирования системы, такие как:

- мониторинг включенности компьютеров в сеть;
- мониторинг системных журналов и журналов безопасности;
- контроль объема доступного дискового пространства;
- мониторинг системных ресурсов сервера;
- контроль над обновлениями антивирусных сигнатур на серверах и рабочих станциях;
- установка критически важных обновлений на сервера и на компьютеры по сети;
- обслуживание сетей в части обеспечения информационной безопасности.

Все это позволит обеспечить высокий уровень надежности при обслуживании компьютеров и серверов, сделать работу сети бесперебойной.

Для исполнения своих должностных обязанностей системные администраторы должны знать:

- системы каталогов Active Directory, серверных и десктопных операционных систем семейства Windows;
- основы построения ЛВС, технологий DNS, DHCP;
- принципы ремонта персональных компьютеров и оргтехники;
- системы организации комплексной защиты информации, способы предупреждения несанкционированного доступа к информации, повреждения или умышленного искажения информации, порядка оформления технической документации;
- аппаратное и программное обеспечение локальных вычислительных сетей.

2.2 Схема сети университета и описание имеющегося оборудования

Топология ЛВС университета представлена головным вузом, расположенным в г. Екатеринбурге и состоящим из нескольких корпусов, а также филиала в г. Нижний Тагил и представительств в др. городах России (рисунок 15). Вся ЛВС университета поделена на отдельные VLAN-ы. Общее количество VLAN — порядка 45. Между филиалом и некоторыми представительствами также организована сеть на базе VLAN.

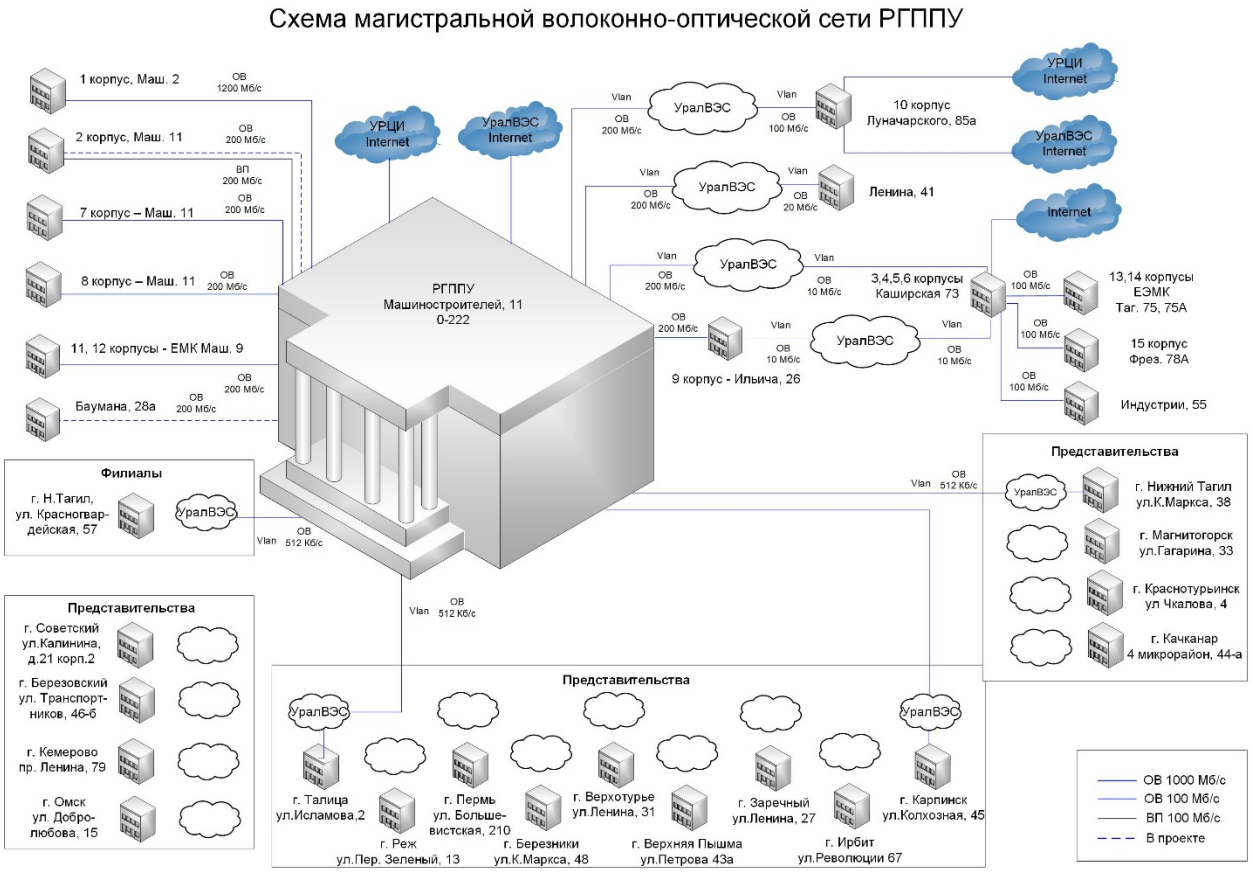


Рисунок 15 — Схема сети университета

Парк ПК университета насчитывает около 600 компьютеров с различными техническими характеристиками. На ПК установлены ОС семейства Microsoft: Windows 7, 8.1, 10.

У университета имеется собственный полностью оборудованный центр обработки данных (ЦОД), представленный на рисунке 16.

Рисунок 16 — Общий вид центра обработки данных

Все оборудование смонтировано в специальный серверный шкаф с климатической сплит-системой Rittal LCP DX.

Для защиты от скачков напряжения, различного рода помех в сети электропитания, а также для обеспечения бесперебойной работы сетевого и серверного оборудования ЦОД в случае кратковременного отключения основного источника, установлен источник бесперебойного питания (ИБП) ABB Upscale RI 11 (рисунок 17).

Рисунок 17 — Внешний вид источника бесперебойного питания

ЦОД представлен физическими серверами формата Rack (10 шт., производители IBM, Aquarius, Intel). Ряд физических серверов входит в виртуальную инфраструктуру VMWare. На серверах установлены ОС: Windows Server 2008 R2, Windows Server 2012 и Windows Server 2016. Для отвода высоких тепловых мощностей из серверного шкафа, а также для эффективного охлаждения, установленного в нем оборудования.

Обслуживание компьютеров производится вручную отделом развития информационных сетей и технического сопровождения.

Обновление серверов производится автоматически посредством центра обновления Windows. На рабочих станциях установка обновлений производится тем же образом. На некоторых станциях автоматическое обновление — отключено. Сервер WSUS университет не использует.

2.3 Политика Active Directory и распределение IP-адресов

Microsoft Active Directory — это служба каталогов, представляющая собой распределенную базу данных, в которой содержится информация обо всех элементах корпоративной информационной среды [25]. Именно с развертки службы каталогов Microsoft Active Directory и начинается построение корпоративной среды. Посредством Microsoft Active Directory происходит идентификация пользователей и приложений в корпоративной среде.

На текущий момент в ЛВС университета осуществляется централизованное управление учетными записями на базе службы каталогов Active Directory. Инфраструктура Active Directory представлена 1 лесом, и 1-м доменом. Всего AD содержит около 1200 учетных записей пользователей.

Сеть университета входит в единый домен «study.rsvpu.ru», что обеспечивает:

1. Хранилище данных доменных служб Active Directory может хранить более миллиона объектов, то есть множество объектов не является причиной создания множества доменов.
2. При реорганизации или переходе пользователей из одного подразделения в другое, их проще перемещать между организационными единицами в пределах одного домена.
3. Отдельным доменом проще управлять, так как для него задействован один набор администраторов и политик домена.
4. Администрировать нужно только один набор контроллеров домена.

5. При необходимости административной автономии используются организационные единицы и на его уровне решаются административные задачи.

6. При необходимости административной изоляции требуется развертывание множества лесов, так как домены не обеспечивают границы административной безопасности.

7. Среда одного домена — наиболее простой сценарий управления групповыми политиками.

8. Объекты групповой политики автоматически реплицируются на все контроллеры при наличии одного домена.

9. Один домен обеспечивает наиболее простую среду проектирования проверки подлинности доступа к ресурсам, при этом не нужно создавать доверительные отношения и назначать доступ к ресурсам для пользователей других доменов. Для назначения доступа к ресурсам имеет смысл использовать одну группу, не конфигурируя группы учетных записей и ресурсов.

10. В одном домене все контроллеры могут являться серверами глобального каталога, при этом не применяются ограничения мастера инфраструктуры (рисунок 18) [26].

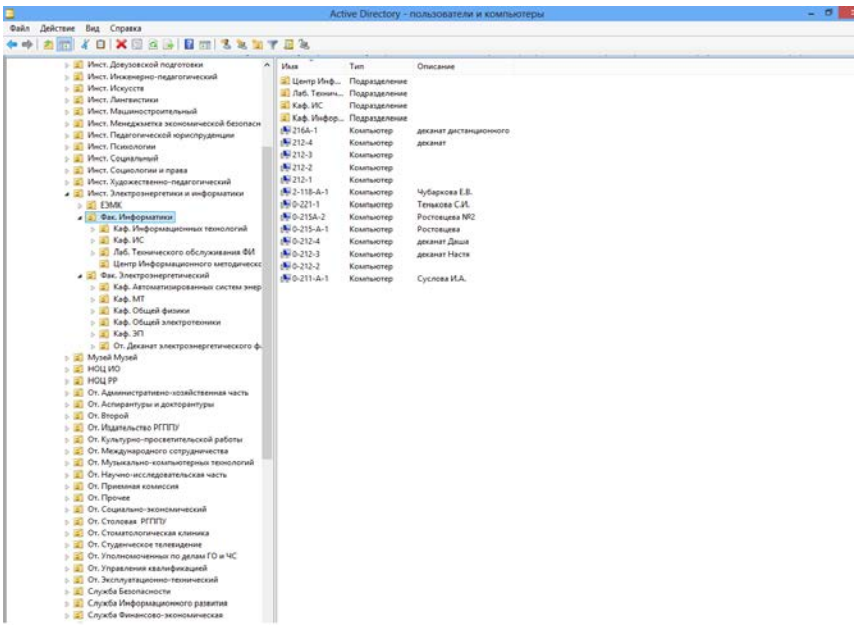


Рисунок 18 — Структура Active Directory

Распределение IP-адресов сетевых устройств производится DHCP-сервером, настроенном на центральном L3 коммутаторе.

2.4 Описание процедуры мониторинга сети с использованием System Center Configuration Manager

В качестве решения для администрирования ИТ-инфраструктуры университетом был выбран программный продукт System Center Configuration Manager как соответствующий необходимым потребностям.

Компьютерный парк университета насчитывает порядка 600 компьютеров. Максимально-возможное количество клиентов и устройств в случае установки автономного первичного сайта составляет 175 000. Соответственно для управления всей инфраструктурой университета будет вполне достаточно одного первичного сайта. В дальнейшем, для достижения высокой доступности и балансировки нагрузки, возможно создание одного или нескольких вторичных сайтов (Secondary Site), либо развертывание дополнительных точек распространения (Distribution Point). Все службы, роли и весь функционал будет расположен на одном виртуальном сервере.

Сотрудники ИТ-отдела университета предоставляют оборудование и программное обеспечение, необходимое для создания Системы, а также выполняют следующие подготовительные работы:

- выделение IP адресов для сетевых интерфейсов сервера и обеспечение их доступности;
- создание виртуальной машины с установленной ОС Windows Server 2016, обновлениями для операционной системы и антивирусным ПО;
- подключение сервера к целевому домену университета;
- обеспечение использования стека протокола TCP/IP всеми серверами, входящими в состав создаваемой системы;

- обеспечение использования единого пространства IP-адресов для создаваемой системы без использования механизма преобразования адресов NAT.

Для осуществления процедуры внедрения продукта Microsoft System Center Configuration Manager, университетом был выделен физический сервер с установленным гипервизором на базе VMware ESXi, 6.7.0 для разворачивания и эксплуатации сервера SCCM 1802. Цель виртуализации сервера SCCM — упрощение процедур архивирования и восстановления системы, а также для возможности использования технологии моментальных снимков во время внедрения.

Предоставляемые аппаратные ресурсы (CPU, память, дисковое пространство) физического сервера могут быть полностью переданы в виртуальную машину для разворачивания системы.

Для развертывания System Center Configuration Manager на платформе виртуализации VMWare VSphere, сотрудниками ИТ-отдела университета была создана виртуальная машина с установленной ОС Windows Server 2016.

Процедура развертывания продукта System Center Configuration Manager состоит из следующих этапов:

1. Проверка готовности сервера к установке SCCM. На данном этапе, производится проверка соответствия сервера минимальным для развертывания SCCM требованиям, а также анализ полученных результатов.
2. Установка платформы NetFramework 3.5, а также включение необходимых ролей и компонентов сервера.
3. Установка инструментов Windows ADK (Windows Assessment and Deployment Kit).
4. Расширение схемы AD.
5. Добавление разрешений на публикацию в AD.
6. Установка и настройка MS SQL сервера.
7. Установка и настройка сервера WSUS (в случае необходимости использования SCUP — точки управления обновлениями).

8. Установка и настройка сервера SCCM.

После развертывания сервера SCCM была проведена предварительная настройка, а именно:

1. Создана группа границ «MAIP Data Center».
2. Установлены и настроены следующие роли сервера:
   - точка Endpoint Protection;
   - точка веб-сайта каталога приложений;
   - точка веб-службы каталога приложений;
   - точка обновления программного обеспечения;
   - точка службы отчетов.
3. Активированы следующие виды обнаружений:
   - обнаружение ресурсов в лесах AD;
   - обнаружение групп AD из OU=MAIP;
   - обнаружение систем AD из OU=Компьютеры, OU=MAIP;
   - обнаружение пользователей AD из OU=РГППУ.
4. Выполнено первичное обнаружение ресурсов (рисунок 19).

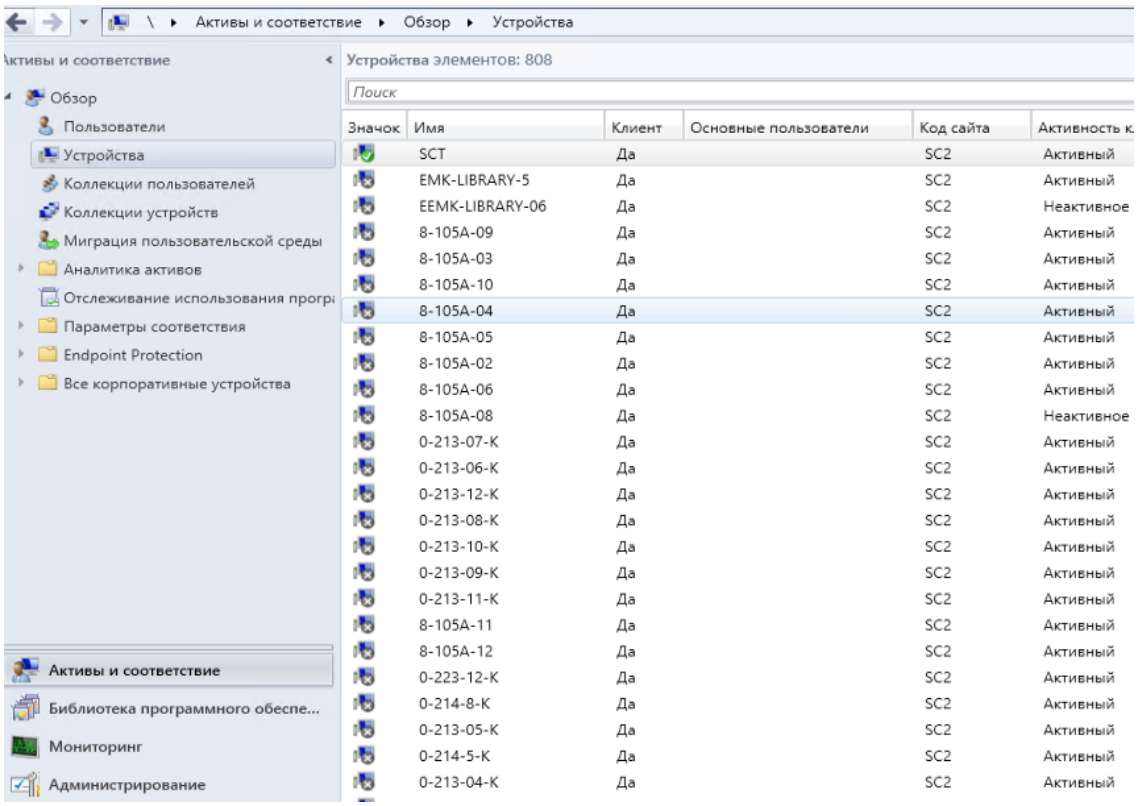


Рисунок 19 — Обнаружение ресурсов в System Center Configuration Manager

5. Настроены параметры клиентов SCCM;

6. Активирована принудительная автоматическая установка клиентов SCCM в пределах AD (рисунок 20).

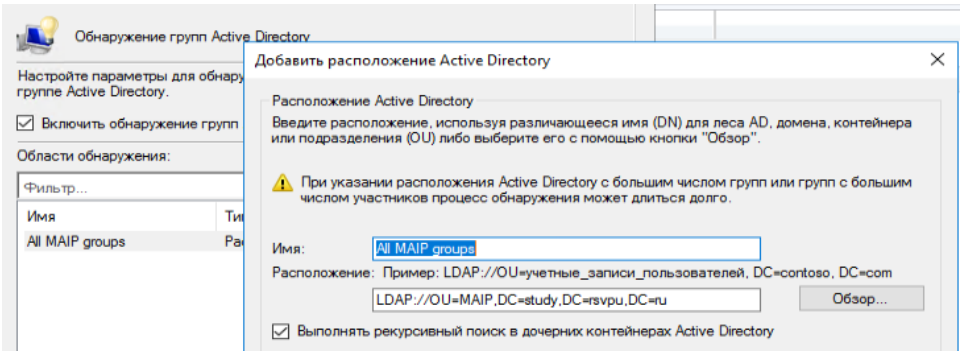


Рисунок 20 — Окно выбора расположения Active Directory

2.5 Описание процедуры администрирования с использованием System Center Configuration Manager

После развёртывания инфраструктуры Configuration Manager логичным продолжением будет установка клиентов SCCM. Configuration Manager предлагает несколько способов развёртывания клиентов. Каждый из них имеет свои плюсы и минусы и в большинстве случаев применяется комбинация из нескольких способов для достижения оптимального результата. Рассмотрим вкратце доступные способы установки и развернём агента SCCM на группе компьютеров.

Клиент SCCM представляет собой ПО, взаимодействующее с серверами сайта. Клиент состоит из различных агентов, которые мы можем включать или выключать, а также настраивать различные параметры работы

Можно создать различные настройки клиентов и привязать их к разным коллекциям, если необходимо.

На найденных системах можно запустить установку клиента вручную с помощью мастера установки клиента или настроить автоматическую установку на все обнаруженные компьютеры. Для этого учётная запись сервера сайта или учётная запись **Client Push installation Account** должны быть чле-

нами локальной группы администраторов на целевой системе. Я создам учётную запись Client Push Installation в Active Directory и включу её в группу Domain Admins для простоты. Но ничего не мешает включить эту учётную запись в группу локальных администраторов на всех необходимых компьютерах с помощью групповой политики.

С помощью консоли были установлены и развернуты:

- средство антивирусной защиты System Center Endpoint Protection;
- обновления операционной системы на рабочих станциях;
- специализированное и офисное программное обеспечение.

2.6 Описание подготовленного образа виртуальной машины

Для осуществления процесса обучения по работе с системой Microsoft System Center Configuration Manager, было подготовлено 2 виртуальных машины на базе платформы виртуализации Microsoft Hyper-V (рисунок 21).

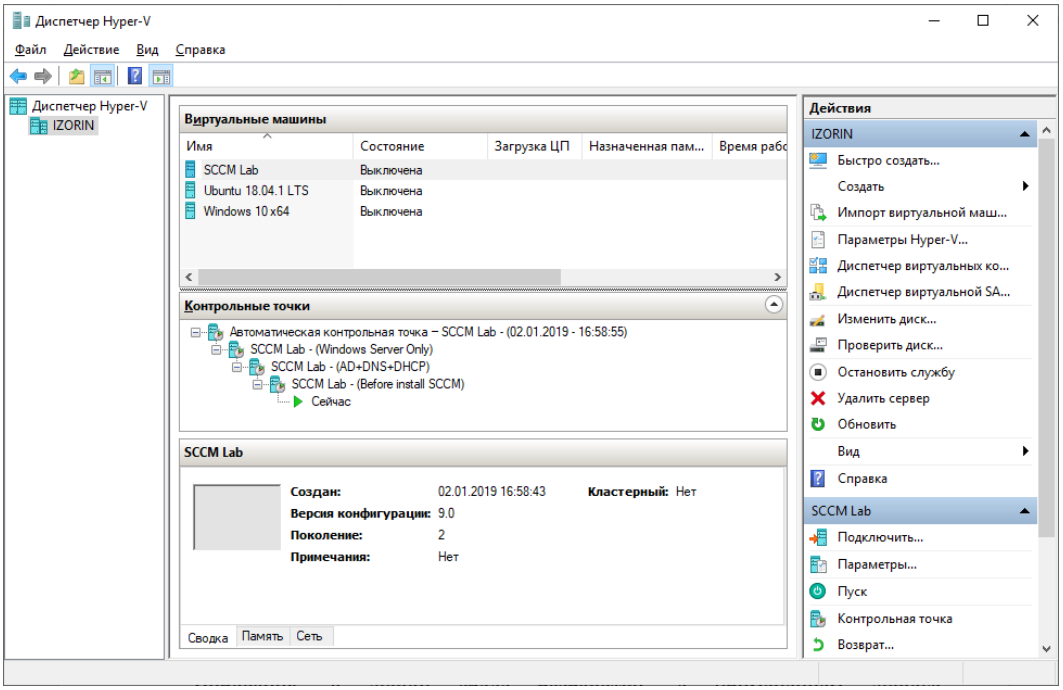


Рисунок 21 — Комплект виртуальных машин в Microsoft Hyper-V

На одной виртуальной машине установлена ОС — Windows 10, на второй — Windows Server 2016. Затем, на виртуальной машине с Windows Server

2016 были развернуты необходимые роли и компоненты Windows Server, а также установлена непосредственно сама система SCCM.

Для возможности самостоятельного развертывания сервера SCCM, а также ролей и компонентов, в процессе создания виртуальной машины были созданы контрольные точки.

2.7 Средство реализации руководства

При помощи Dr.Explain можно легко создавать документацию как для обычных, так и онлайн-приложений, написанных на любом языке программирования, в любой среде разработки, с применением любого NET.Framework.

Dr.Explain автоматически создает аннотированные скриншоты с нумерованными выносками и метками. По сравнению с другими инструментами создания справок, эта уникальная технология позволяет гораздо быстрее создавать документацию для приложений со сложными интерфейсами. Это самый эффективный способ создания справок, руководств и печатной документации

В данной программе с легкостью можно управлять текстами, техническими иллюстрациями и аннотированными скриншотами, задавать гибкую структуру документа, контента и разделов, встраивать поддержку индексов ключевых слов и возможность полнотекстового поиска без программирования или создания скриптов на стороне сервера, связывать разделы с модулями приложений для создания контекстно-зависимых справок. Dr.Explain поддерживает множество форматов вывода для единого источника информации.

В данной программе можно использовать один источник и один инструмент для создания файлов помощи, онлайн-руководств или готовой к печати документации для любого программного обеспечения. Можно генерировать онлайн-руководства со встроенным поиском без использования программирования, баз данных или скриптов. Также можно компилировать фай-

лы помощи в формате Microsoft HTML в формат CHM для включения их в пакет поставки вашего ПО. Создавать готовую к печати кроссплатформенную документацию в форматах RTF и PDF.

2.8 Основные разделы руководства

Раздел «Основная задача руководства». Руководство по мониторингу и администрированию сети университета средствами System Center Configuration Manager даёт представление об использовании Configuration Manager и связанных с ним систем сайта для эффективного управления ресурсами сети, а также управлении приложениями, мониторинге «здоровья» клиентов, инвентаризации аппаратного и программного обеспечения, развертывании операционных систем и обновлении программного обеспечения (рисунок 22). Также данное руководство рассматривает задачи, связанные с настройкой и работой System Center Forefront Endpoint Protection, управлением соответствиями, созданием запросов и отчётов.

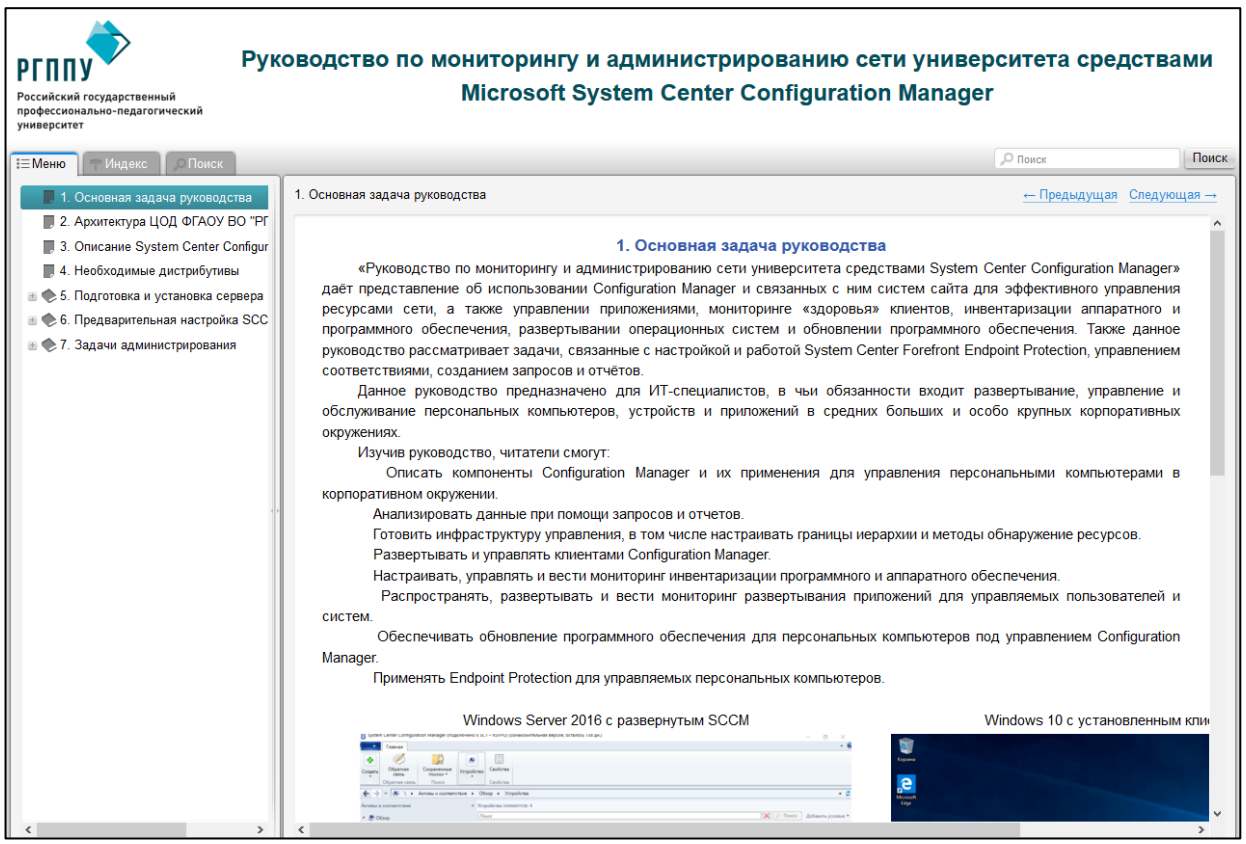


Рисунок 22 — Руководство по мониторингу и администрированию сети университета средствами System Center Configuration Manager

Данное руководство предназначено для ИТ-специалистов, в чьи обязанности входит развертывание, управление и обслуживание персональных компьютеров, устройств и приложений в средних больших и особо крупных корпоративных окружениях.

Изучив руководство, ИТ-специалисты смогут:

- описать компоненты Configuration Manager и их применения для управления персональными компьютерами в корпоративном окружении;
- анализировать данные при помощи запросов и отчетов;
- готовить инфраструктуру управления, в том числе настраивать границы иерархии и методы обнаружение ресурсов;
- развертывать и управлять клиентами Configuration Manager;
- настраивать, управлять и вести мониторинг инвентаризации программного и аппаратного обеспечения;
- распространять, развертывать и вести мониторинг развертывания приложений для управляемых пользователей и систем;
- обеспечивать обновление программного обеспечения для персональных компьютеров под управлением Configuration Manager;
- применять Endpoint Protection для управляемых персональных компьютеров.

В разделе **«Архитектура ЦОД РГППУ»** содержится общее описание компонентов ЦОД РГППУ. Приведены характеристики этих компонентов. Так же разобран принцип работы и способы управления климатической системой Rirtal LCP DX (рисунок 23).

Помимо этого, в разделе представлена общая схема магистрально волоконно-оптической сети РГППУ, на которой обозначены все корпуса головного вуза, а также филиалы и представительства вуза, с указанием скоростей соединения.

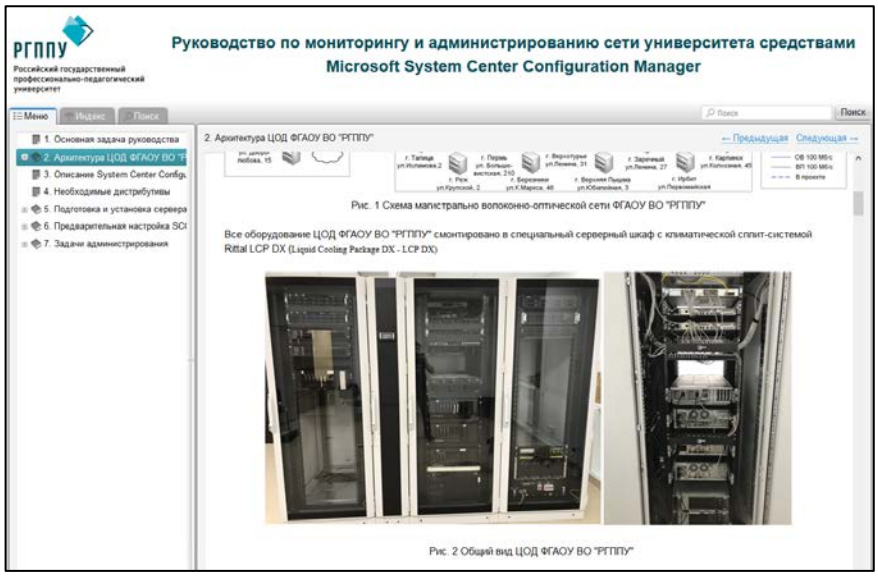


Рисунок 23 — Раздел руководства «Архитектура ЦОД РГППУ»

Раздел **«Описание System Center Configuration Manager»** содержит описание пакета продуктов System Center и непосредственно продукта Configuration Manager (рисунок 24). Так же перечислены возможные топологии иерархии сайтов и приведено описание всех возможных ролей системы

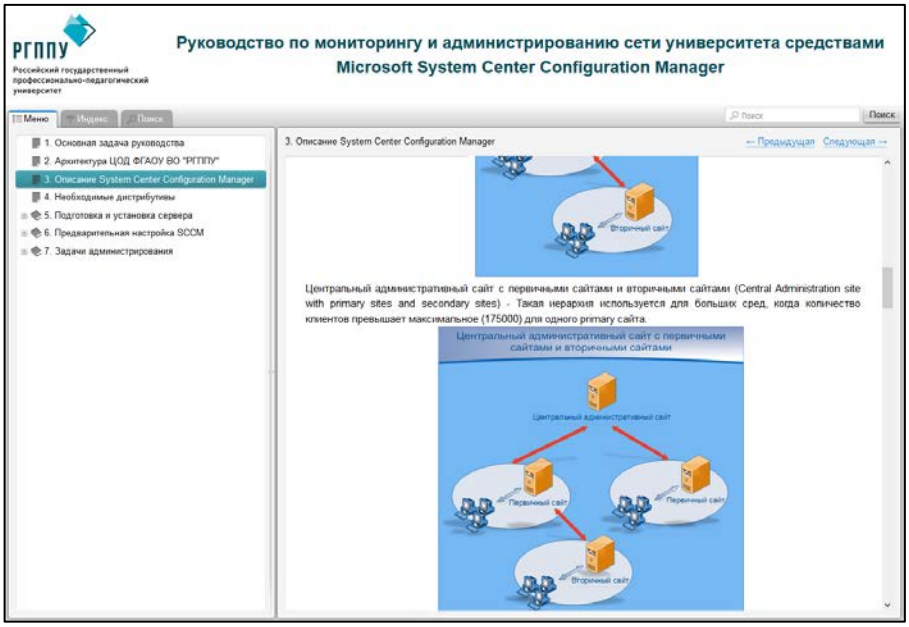


Рисунок 24 — Раздел руководства «Описание System Center Configuration Manager»

В разделе **«Необходимые дистрибутивы»** представлены различные варианты получения необходимых дистрибутивов (рисунок 25).

А именно:

1. Volume Licensing Service Center (VLSC) — при наличии приобретенной платной подписки Microsoft.
2. Подписка Microsoft Azure.
3. Ознакомительные версии (180 дней).

Рассмотрены варианты получения дистрибутивов (сервисов) как для использования в обучении, так и для установки в организации.

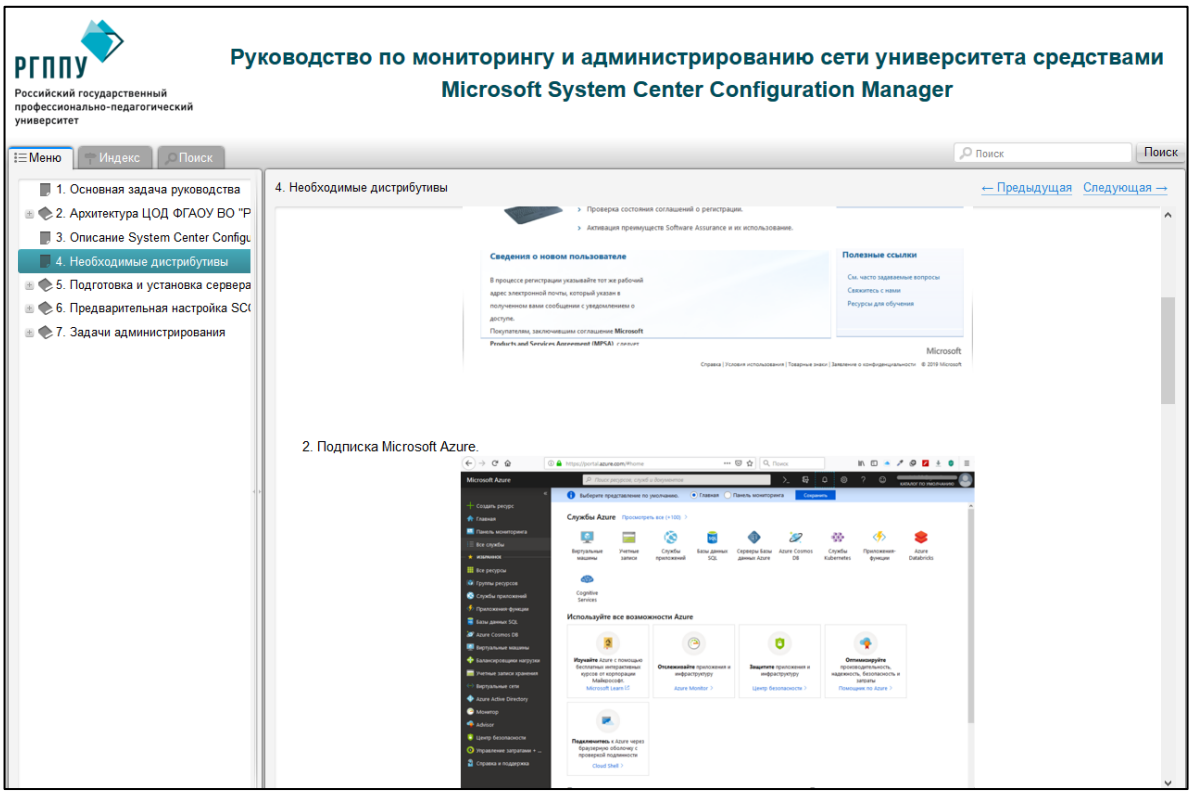


Рисунок 25 — Раздел руководства «Необходимые дистрибутивы»

Раздел **«Подготовка и установка сервера SCCM»** руководства содержит подробные сведения о предварительной подготовке оборудования к установке сервера MS SCCM (рисунок 26). Приведены рекомендуемые характеристики оборудования для установки сервера SCCM. В подразделах описывается процесс создания и настройки виртуальной машины для последующего развертывания системы SCCM. Рассматривается два варианта создания виртуальных машин:

- в среде виртуализации Microsoft Hyper-V;
- на платформе виртуализации VMWare VSphere.

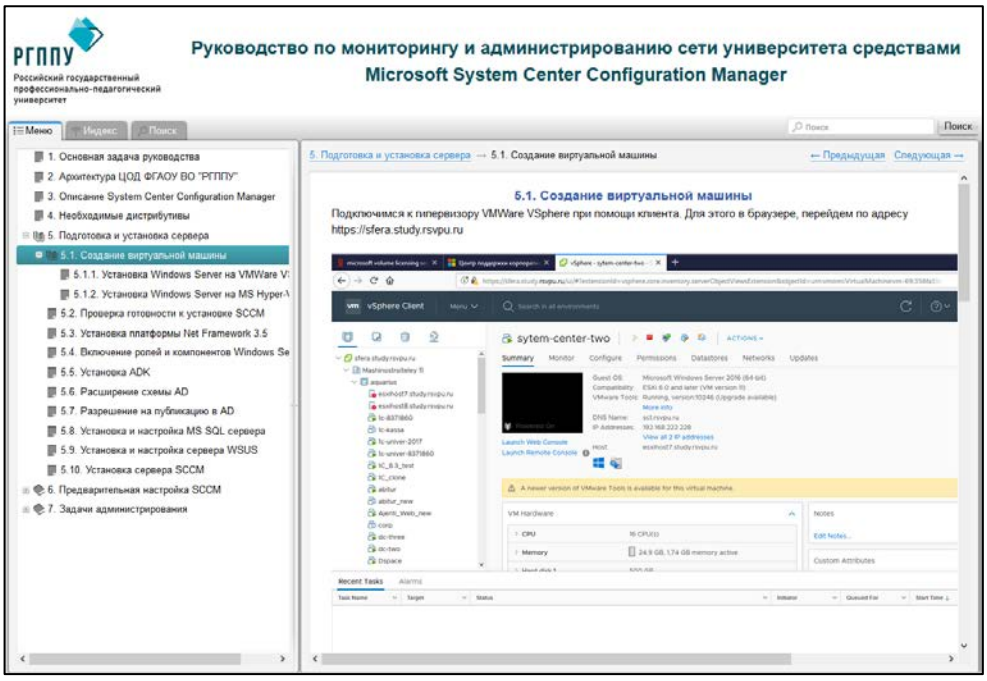


Рисунок 26 — Раздел руководства «Подготовка и установка сервера»

Помимо создания самих виртуальной машины, содержится информация по установке операционной системы на нее.

Так же, последовательно описаны этапы предварительной настройки операционной системы. А именно:

- установка платформы .NET Framework 3.5;
- включение необходимых ролей и компонентов Windows Server;
- установка средств для развертывания и оценки Windows ADK;
- расширение схемы Active Directory;
- разрешение на публикацию в Active Directory.

Заключительные подразделы содержат подробное описание процесса установки и настройки сервера MS SQL, сервера WSUS. Также подробно описан процесс установки непосредственно самого сервера Microsoft System Center Configuration Manager версии 1802.

В разделе **«Предварительная настройка SCCM»** содержится информация по предварительной настройке вновь установленного сервера SCCM (рисунок 27). А именно:

- создание границ;
- настройка методов обнаружения;

- настройка ролей системы;
- настройка автоматического развертывания клиентов SCCM на рабочие станции в домене.

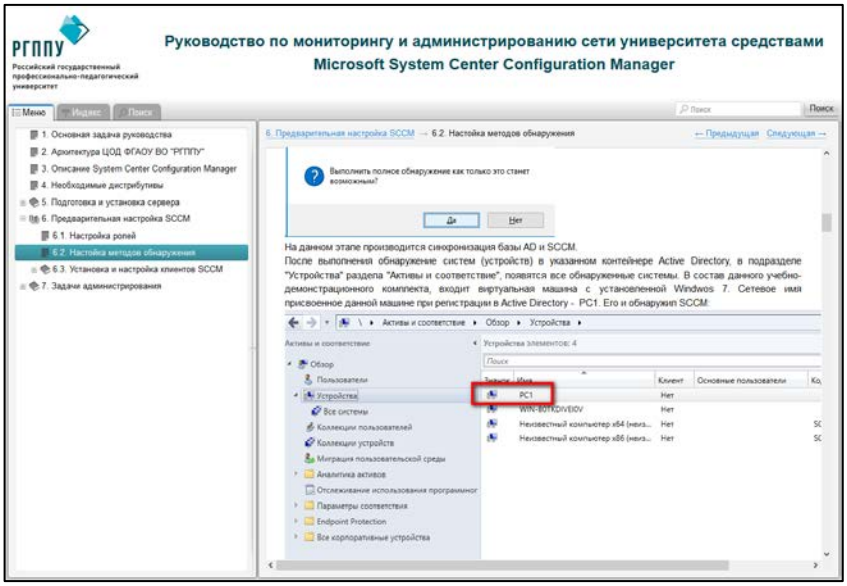


Рисунок 27 — Раздел руководства «Предварительная настройка SCCM»

В разделе **«Задачи администрирования»** подробно описываются основные задачи администрирования, выполняемые посредством SCCM. А именно:

1. Работа с консолью SCCM (рисунок 28). Данный раздел руководства содержит основную информацию о консоли SCCM, ее назначении, требованиях к установке, а также описание интерфейса.

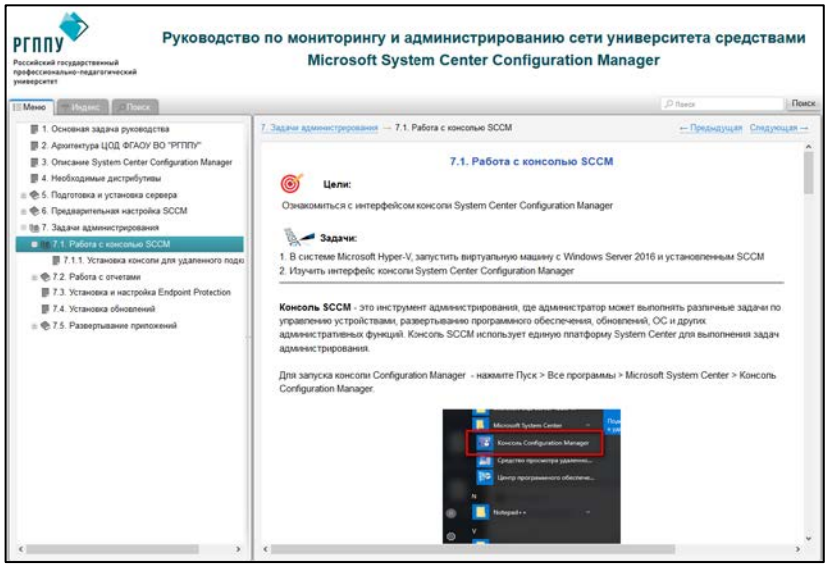


Рисунок 28 — Раздел «Работа с консолью SCCM»

2. Работа с отчетами (рисунок 29). Данный раздел руководства содержит инструкции по установке и настройке точки служб отчетов, работе как со встроенными в SCCM отчетами, так и созданию своих собственных отчетов в конструкторе отчетов Microsoft SQL Server Report Builder при помощи SQL-запросов. Помимо описания работы с отчетами, в данном разделе имеется ряд практических примеров SQL-запросов.

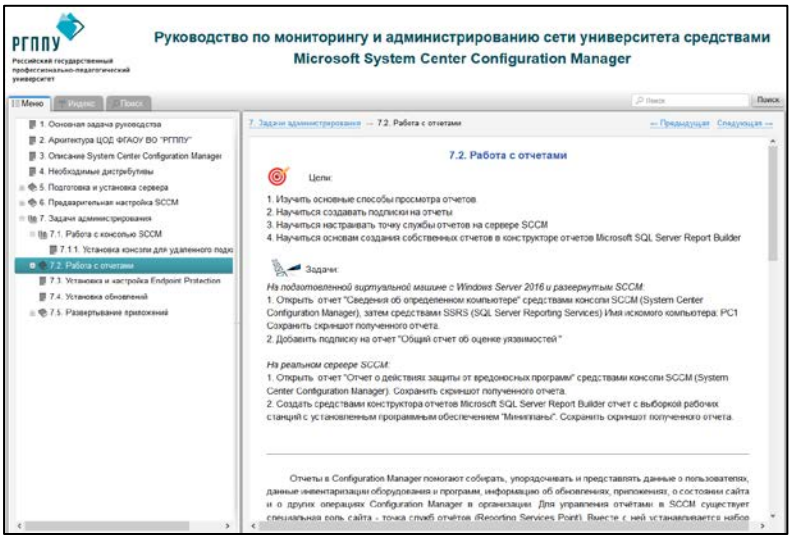


Рисунок 29 — Раздел «Работа с отчетами»

3. Установка и настройка System Center Endpoint Protection (SCEP) (рисунок 30). Данный раздел содержит информацию по установке антивирусного программного обеспечения Microsoft Forefront Endpoint Protection, настройке политик защиты от вредоносного ПО, а также осуществление мониторинга.

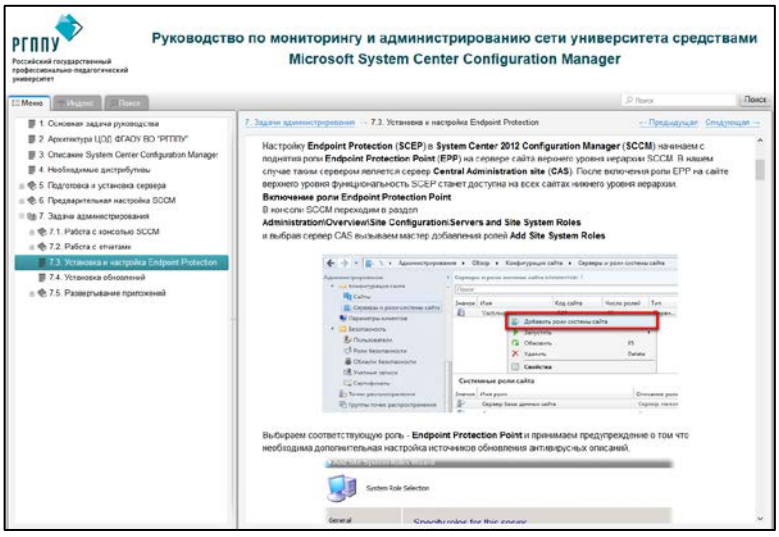


Рисунок 30 — Установка и настройка Endpoint Protection

4. Установка обновлений (рисунок 31). В данном разделе содержится информация по настройке развертывания обновлений Windows на клиентах SCCM, а также мониторингу состояния развертывания.

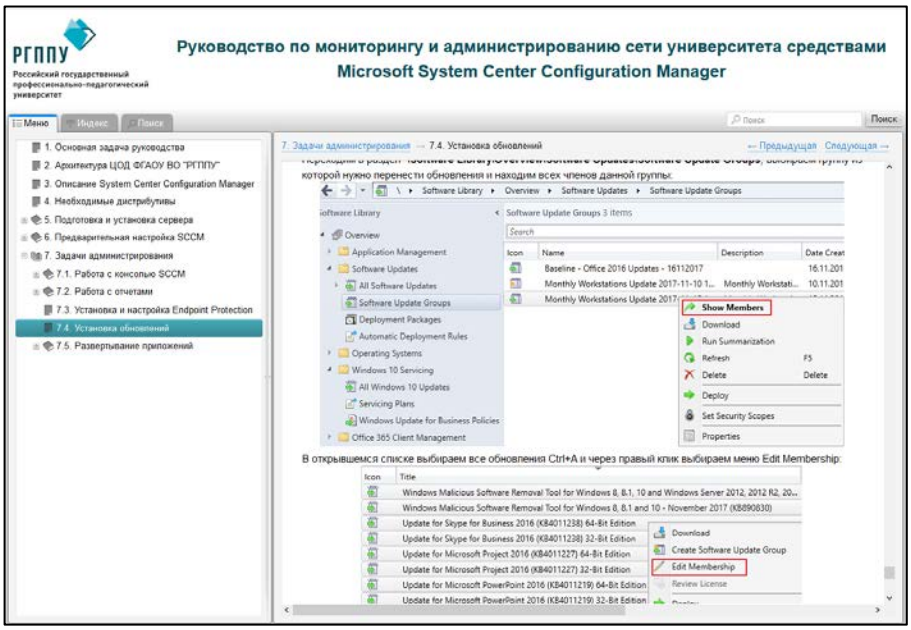


Рисунок 31 — Установка обновлений

5. Развертывание приложений (рисунок 32). Данный раздел описывает процедуру развертывания приложений при помощи SCCM. В качестве примера рассмотрено развертывания приложения MS Office 2016.

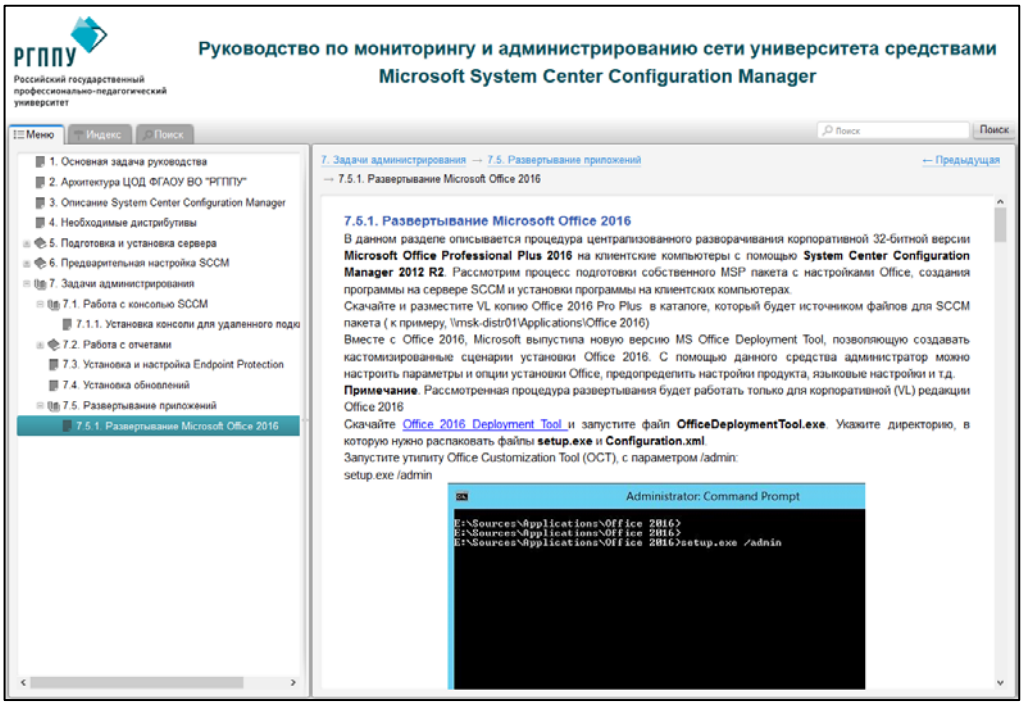


Рисунок 32 — Раздел «Развертывание приложений»

В каждой задаче администрирования четко сформулированы достигаемые цели, имеются практические задания и ряд вопросов для самопроверки.

2.9 Организация процесса обучения сотрудников с использованием руководства

Процесс обучения сотрудников ИТ-отдела разбит 2 части:

1. Обучение развертыванию и настройке SCCM:

- изучается руководство по мониторингу и администрированию сети университета средствами System Center Configuration Manager;
- на рабочей станции, с установленной операционной системой Windows 10 или Windows Server 2016 и включенной ролью Hyper-V, разворачивается 2 виртуальные машины. Одна виртуальная машина с ОС Windows Server 2016, вторая — с ОС Windows 10;
- на виртуальной машине с Windwos Server 2016 выполняется поэтапное развертывание системы SCCM согласно разделам 5-6 данного руководства;
- на виртуальной машине с Windows 10 устанавливается клиент SCCM.

2. Обучение основам работы с SCCM:

- изучается руководство по мониторингу и администрированию сети университета средствами System Center Configuration Manager;
- на рабочей станции, с установленной операционной системой Windows 10 или Windows Server 2016 и включенной ролью Hyper-V, разворачивается 2 виртуальные машины. Одна виртуальная машина с ОС Windows Server 2016, вторая — с ОС Windows 10;
- изучается интерфейс MS SCCM;
- выполняются задания из раздела 7 — «Задачи администрирования» руководства.

Первая часть позволяет освоить установку и настройки MS SCCM «с нуля». Вторая часть — знакомит с интерфейсом SCCM и основными задачами администрирования.

ЗАКЛЮЧЕНИЕ

Программы мониторинга уже давно используются в больших и малых компаниях для облегчения работы системных администраторов и повышения безопасности локальной сети.

Многообразие программ мониторинга на рынке позволяет подобрать абсолютно любое решение, как платное, так и бесплатное, на вкус даже самого придирчивого пользователя, поэтому не пользоваться их функционалом, лишь усложнять себе жизнь, затрачивая гораздо больше времени на работу, ставя неправильные диагноз и пропуская атаки злоумышленников.

В ходе выпускной квалификационной работы был проведен анализ исходных данных в сфере IT-аудита и мониторинга компьютерных сетей; существующих программ сетевого мониторинга. На основании проведенного анализа, выбран продукт MS SCCM — как отвечающий необходимым требованиям и потребностям университета. Затем совместно с сотрудниками ИТ-отдела, выбранный продукт был развернут на оборудовании университета. Были произведены основные настройки согласно требующимся задачам и выполнено тестирование функций системы.

С помощью SCCM 1802 университет планирует управлять 500 рабочими станциями и 10 физическими серверами, 5 из которых однопроцессорных, 5 двухпроцессорных. Для этих целей университет предоставляет следующий набор лицензий Microsoft:

После чего были разработаны обучающие инструкции по работе с системой MS SCCM.

Руководство по управлению ИТ-инфраструктурой при помощи Microsoft System Center Configuration Manager даёт представление об использовании Configuration Manager и связанных с ним систем сайта для эффективного управления ресурсами сети, а также управлении приложениями, мониторинге «здоровья» клиентов, инвентаризации аппаратного и программного

обеспечения, развертывании операционных систем и обновлении программного обеспечения. Также данное руководство рассматривает задачи, связанные с настройкой и работой System Center Endpoint Protection, управлением соответствиями, созданием запросов и отчётов. Обучение проводится очно в оборудованных классах, либо непосредственно на рабочих местах.

Всё это обеспечивает возможности:

- мониторинга работы рабочих станций и серверов в сети;
- развертывания программного обеспечения на рабочих станциях и серверах;
- сбора инвентаризационных данных об аппаратном и программном обеспечении (Приложение А);
- контроля над обновлениями антивирусных сигнатур на серверах и рабочих станциях;
- установки критически важных обновлений на сервера и на компьютеры по сети (Приложение В);
- защиты рабочих станций и серверов от вредоносного программного обеспечения (Приложение Г).

Актуальность данной работы состоит в том, что обучение специалистов в области информационных технологий (ИТ-специалистов) для сопровождения Microsoft System Center происходит только на дорогих узко квалифицированных курсах. Помимо этого, на подобного рода курсах рассматриваются общие схемы и принципы внедрения продуктов семейства MS SCCM, без учета специфики конкретной организации, в которой работает сотрудник. Разработка данного руководства позволит снизить затраты на обучение будущих сотрудников работе с MS SCCM, а также передать имеющийся опыт работы с данной системой.

Таким образом, все поставленные задачи были выполнены, а цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Аудит компьютерной сети [Электронный ресурс]. — Режим доступа: http://www.h20.ru/admin-netaudit.php (дата обращения: 08.05.2019).

2. Аудит сети [Электронный ресурс]. — Режим доступа: http://www.smbtelecom.ru/content/50/uslugi-po-postroeniyu-setei/audit-setei (дата обращения: 09.01.2019).

3. Бесплатные программы для работы с сетью [Электронный ресурс]. — Режим доступа: http://ab57.ru/netsoft.html (дата обращения: 07.01.2019).

4. Блог об актуальных IT-технологиях для построения современной IT-инфраструктуры [Электронный ресурс]. — Режим доступа: https://itblog.ru.net (дата обращения: 04.01.2019).

5. Блог о SCCM [Электронный ресурс]. — Режим доступа: https://masyan.ru/category/sccm (дата обращения: 08.01.2019).

6. Брагинский А. Локальные сети. Модернизация и поиск неисправностей [Текст]: учебное пособие / А. Брагинский — Санкт-Петербург: БХВ-Петербург, 2012. — 832 с.

7. Енюков И. Статистический анализ и мониторинг научно-образовательных интернет-сетей [Текст]: учебное пособие / И. Енюков, И. Ретинская, А. Сакуратов. — Санкт-Петербург: БХВ-Петербург, 2010. — 320 с.

8. Кенин А. Самоучитель системного администратора [Текст]: учебное пособие / А. Кенин. — Санкт-Петербург: БХВ-Петербург, 2012. — 512 с.

9. Кристофер Н. Ubuntu и Debian Linux для продвинутых. Более 1000 незаменимых команд [Текст]: учебное пособие / Н. Кристофер, К. Франсуа. — Санкт-Петербург: Питер, 2010. — 352 с.

10. Лекции по системам и сетям [Электронный ресурс]. — Режим доступа: http://seticom.narod.ru/lit/12sdl-01.htm#31 (дата обращения: 12.02.2019).

11. Мониторинг и анализ компьютерных сетей [Электронный ресурс]. — Режим доступа: http://www.sharovt.narod.ru/l23.htm (дата обращения: 13.01.2019).

12. Мониторинг и управление компонентами IT-структуры [Электронный ресурс]. — Режим доступа: http://www.topsbi.ru/?trID=141 (дата обращения: 09.01.2019).

13. Мэлоун Д. IPv6. Администрирование сетей [Текст]: учебное пособие / Д. Мэлоун. — Санкт-Петербург: КУДИЦ-Пресс, 2010. — 320 с.

14. Официальный сайт программы zabbix [Электронный ресурс]. — Режим доступа: http://www.zabbix.com/ (дата обращения: 15.02.2019).

15. Полезные программы для Friendly Pinger [Электронный ресурс]. — Режим доступа: http://susl-ik.blogspot.ru/2013/10/friendly-pinger-external-commands.html (дата обращения: 20.01.2019).

16. Пользователи, группы и права доступа [Электронный ресурс]. — Режим доступа: http://help.ubuntu.ru/manual/пользователи_и_группы (дата обращения: 18.01.2019).

17. Пульт управления локальной сетью [Электронный ресурс]. — Режим доступа: http://white55.narod.ru/fpinger.html (дата обращения: 24.01.2019).

18. Смирнова Е. Технологии современных сетей Ethernet [Текст]: учебное пособие / Е. Смирнова. — Санкт-Петербург: БХВ-Петербург, 2012. — 272 с.

19. Трулов Д. Сети. Технологии, прокладка, обслуживание [Текст]: учебное пособие / Д. Трулов. — Москва: НТ Пресс, 2012 г. — 560 с.

20. Уилсон Э. Мониторинг и Анализ сетей [Текст]: учебное пособие / Э. Уилсон. — Москва: Лори, 2010. — 350 с.

21. Управление компьютерной сетью [Электронный ресурс]. — Режим доступа: http://ru.wikipedia.org/wiki/Управление_компьютерной_сетью (дата обращения: 18.02.2019).

22. Утилита PsTools [Электронный ресурс]. — Режим доступа: http://technet.microsoft.com/ru-ru/sysinternals/bb896649.aspx (дата обращения: 05.01.2019).

23. Форум на Kuban.ru — Решения для локальной сети [Электронный ресурс]. — Режим доступа: http://forums.kuban.ru/f1029/kakoe_reshenie_dlya_lokalki_vybrat--2098094.html (дата обращения: 27.01.2019).

24. Хабракен Д. Маршрутизаторы Cisco. Практическое применение [Текст]: учебное пособие / Д. Хабракен, М. Крелл. — Санкт-Петербург: БХВ-Петербург, 2012. — 316 с.

25. Active Directory [Электронный ресурс]. — Режим доступа: http://ru.wikipedia.org/wiki/Active_Directory (дата обращения: 13.01.2019).

26. Active Directory. От простого к сложному [Электронный ресурс]. — Режим доступа: http://alterego.ucoz.org/publ/windows_server/ad1/3-1-0-30 (дата обращения: 08.02.2019).

27. Bitcoin Forum — Удаленное включение компьютера [Электронный ресурс]. — Режим доступа: https://forum.btcsec.com/index.php?/blog/28/entry-33-udalennoe-vkliuchenie-kompiutera/ (дата обращения: 08.02.2019).

28. Depicus Wake On Lan command line [Электронный ресурс]. — Режим доступа: http://www.depicus.com/wake-on-lan/wake-on-lan-cmd.aspx (дата обращения: 15.06.2019).

29. Free ebook: Microsoft System Center: Troubleshooting Configuration Manager [Электронный ресурс]. — Режим доступа: https://blogs.msdn.microsoft.com/microsoft_press/2013/11/12/free-ebook-microsoft-system-center-troubleshooting-configuration-manager/ (дата обращения: 04.01.2019).

30. Friendly pinger о программе [Электронный ресурс]. — Режим доступа: http://www.kilievich.com/rus/fpinger/ (дата обращения: 07.01.2019).

31. Friendly Pinger. Компьютерная помощь [Электронный ресурс]. — Режим доступа: http://forum.ru-board.com/topic.cgi?forum=5&topic=3553&-start=40 (дата обращения: 13.01.2019).

32. Kerrie Meyler System Center 2012 Configuration Manager Unleashed / Kerrie Meyler, Byron Holt, Marcus Oh, Jason Sandys, Greg Ramsey. — USA: Sams, 2012. — 1360 с.

33. Martyn Coupland Microsoft System Center Configuration Manager Advanced Deployment / Martyn Coupland. — Birmingham, UK: Packet Publishing Ltd, 2014. — 290 с.

34. RealVns — deployment strategies [Электронный ресурс]. — Режим доступа: http://www.realvnc.com/products/vnc/deployment/ (дата обращения: 07.01.2019).

35. System Center Configuration Manager и как с ним бороться [Электронный ресурс]. — Режим доступа: http://liashov.com (дата обращения: 17.01.2019).

36. Vangel Krstevski Mastering System Center Configuration Manager / Vangel Krstevski. — Birmingham, UK: Packet Publishing Ltd, 2014. — 278 с.

ПРИЛОЖЕНИЕ А

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

Институт инженерно-педагогического образования

Кафедра информационных систем и технологий

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль «Информатика и вычислительная техника»

Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
И.о заведующего кафедрой

_____ И.А. Суслова
подпись и.о. фамилия

« 26 » ноября 2019 г.

ЗАДАНИЕ
на выполнение выпускной квалификационной работы бакалавра

студента (ки) ***5*** курса группы *ЗИБ-501*
Зорина Ивана Сергеевича
фамилия, имя, отчество полностью

1. Тема **Мониторинг и администрирование сети университета средствами System Center Configuration Manager**

утверждена распоряжением по институту от «20» сентября 2018 г. № 20-2/10

2. Руководитель ***Ченушкина Светлана Владимировна***
фамилия, имя, отчество полностью

_____ _____ *старший преподаватель* *РГППУ*
ученая степень ученое звание должность место работы

3. Место преддипломной практики *ФГАОУ ВО «РГППУ»*

4. Исходные данные к ВКР *Мэлоун Д. IPv6. Администрирование сетей*
Уилсон Э. Мониторинг и Анализ сетей
Kerrie Meyler System Center 2012 Configuration Manager Unleashed
Martyn Coupland Microsoft System Center Configuration Manager Advanced Deployment

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)

5.1. Анализ источников и представленных на рынке программных решений по мониторингу и администрированию сети

5.2. Настройка программного комплекса и проведение мониторинга компьютерной сети

5.3. Настройка возможности удаленного администрирования серверов и рабочих станций с использованием программного комплекса

5.4. Подготовка обучающих инструкций по работе с комплексом

5.5. Реализация интерфейса руководства в выбранных средствах реализации

6. Перечень демонстрационных материалов *презентация выполненная в MS Power Point, Электронные инструкции*

7. Календарный план выполнения выпускной квалификационной работы

№ п/п	Наименование этапа дипломной работы	Срок выполнения этапа	Процент выполнения ВКР	Отметка руководителя о выполнении
1	Поиск информации по теме ВКР Работа над теоретическим разделом ВКР Сдача зачета по преддипломной практике	12.12.2018	10%	подпись
2	Выполнение работ по разрабатываемым вопросам, их изложение в пояснительной записке ВКР: • анализ источников и представленных на рынке программных решений по мониторингу и администрированию сети; • настройка программного комплекса и проведение мониторинга компьютерной сети; • настройка возможности удаленного администрирования серверов и рабочих станций с использованием программного комплекса; • подготовка обучающих инструкций по работе с комплексом; • реализация интерфейса руководства в выбранных средствах реализации.	28.18.2018	60%	подпись
3	Оформление демонстрационных материалов: электронная презентация (плакаты) и подготовка доклада к предварительной защите	07.01.2019	10%	подпись
4	Нормоконтроль	15.02.2019	10%	подпись
5	Предварительная защита	22.02.2019	10%	подпись
6	Получение рецензии, подготовка к защите ГЭК	22.02.2019	5%	подпись

8. Консультанты по разделам выпускной квалификационной работы

Наименование раздела	Консультант	Задание выдал		Задание принял	
		подпись	дата	подпись	дата

Руководитель _____ _____ *Задание получил* _____ _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить ***Зорина И.С.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.

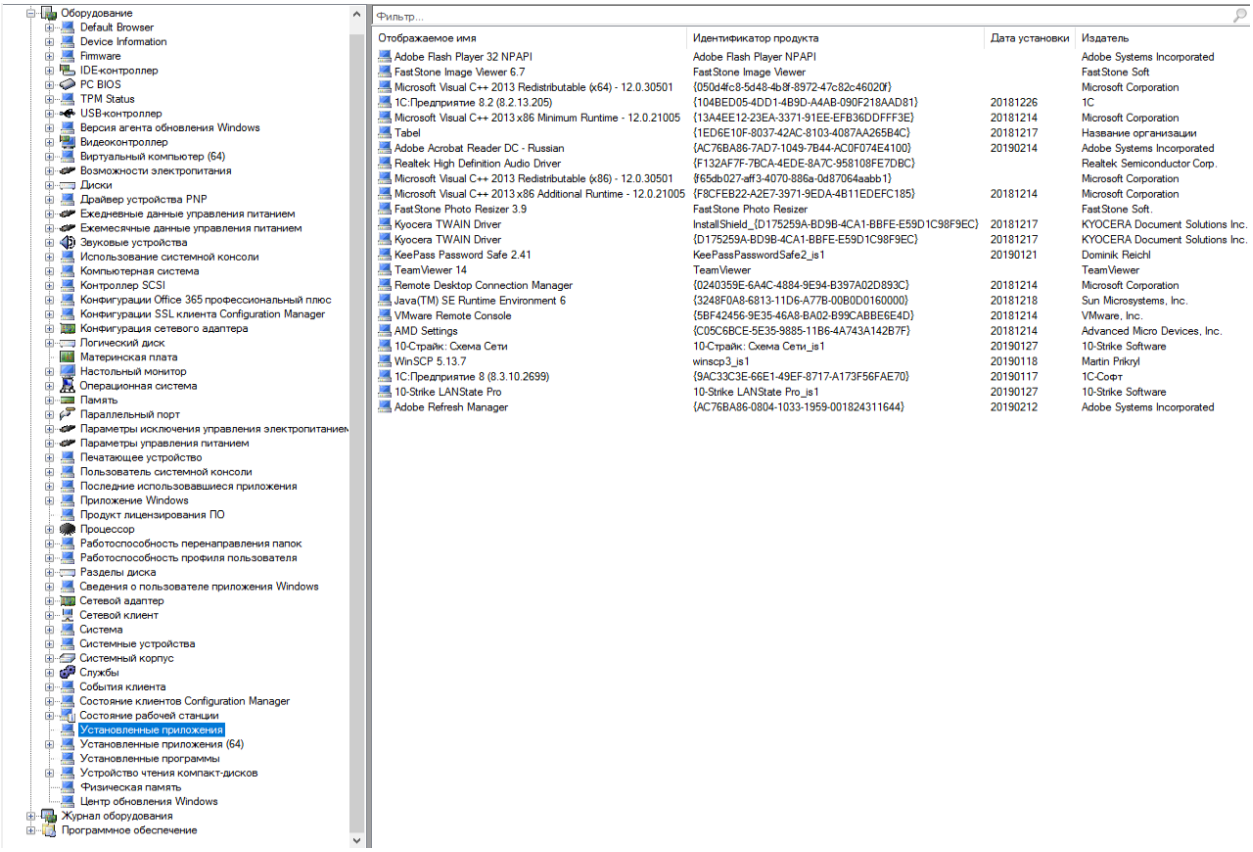
Руководитель _____ _____
подпись дата

10. Допустить ***Зорина И.С.*** к защите выпускной квалификационной работы
фамилия и. о. студента

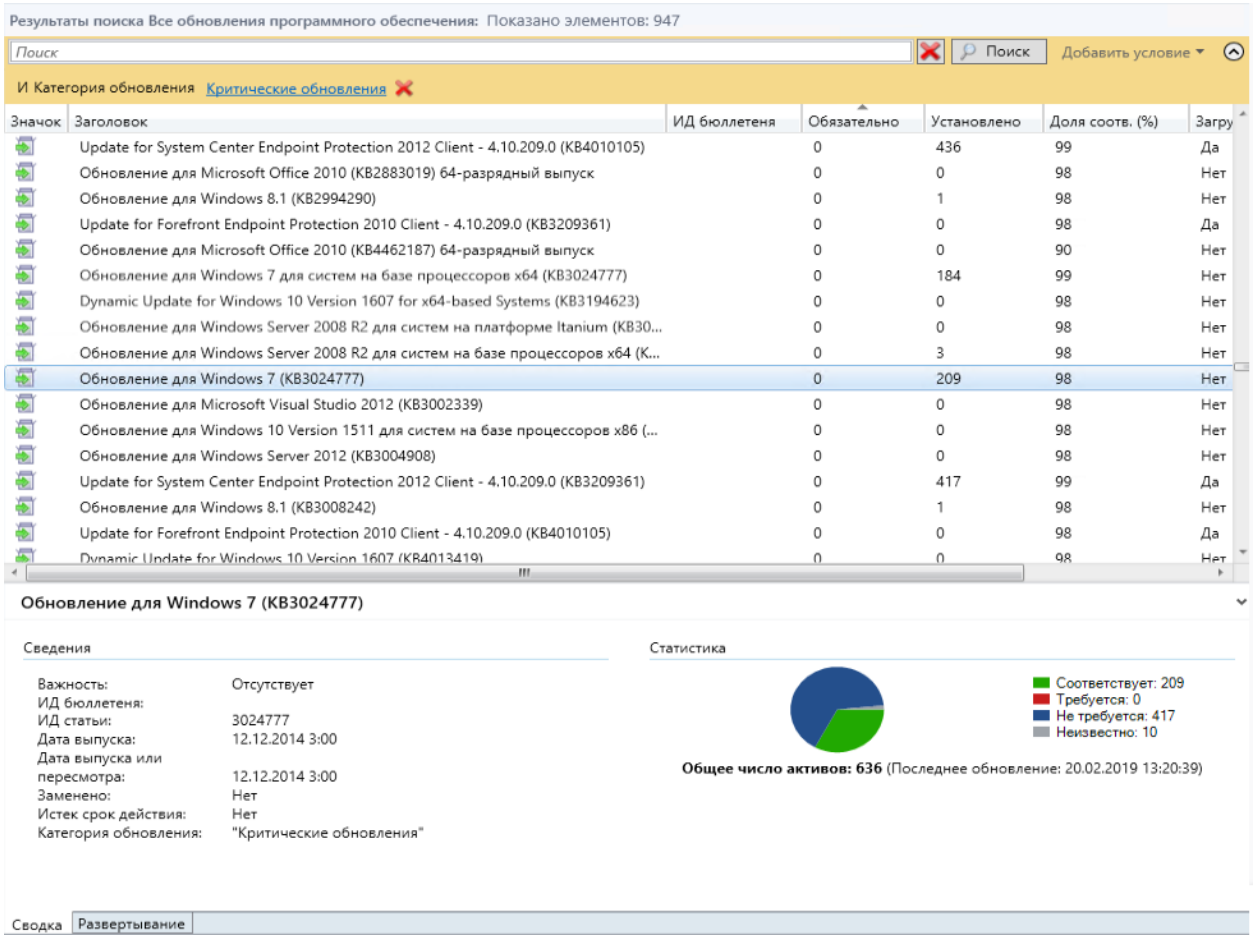
в государственной экзаменационной комиссии (протокол заседания кафедры от «13» февраля 2019 г., № 7)

Заведующий кафедрой _____ _____
подпись дата

ПРИЛОЖЕНИЕ Б



ПРИЛОЖЕНИЕ В



ПРИЛОЖЕНИЕ Г